

A NOVEL ANALYSIS OF HYBRID AND EFFICIENT INTRUSION DETECTION SYSTEMS IN WIRELESS SENSOR NETWORKS

Submitted in partial fulfillment of the requirements for the award of Bachelor of
Engineering degree in Electronics and Communication Engineering

By

SEELAM SUDHEER KUMAR REDDY (37130364)



**DEPARTMENT OF ELECTRONICS AND COMMUNICATION
ENGINEERING SCHOOL OF ELECTRICAL AND ELECTRONICS
ENGINEERING**

SATHYABAMA

**INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)**

Accredited with Grade "A" by NAAC

JEPPIAAR NAGAR, RAJIV GANDHI SALAI, CHENNAI - 600 119

APRIL - 2021



SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY

(DEEMED TO BE UNIVERSITY)

Accredited "A" Grade by NAAC | 12B Status by UGC | Approved by AICTE

www.sathyabama.ac.in

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

BONAFIDE CERTIFICATE

This is to certify that this Project Report is the bonafide work of **SEELAM SUDHEER KUMAR REDDY (37130364)** who carried out the project entitled **A NOVEL ANALYSIS OF HYBRID AND EFFICIENT INTRUSION DETECTION SYSTEMS IN WIRELESS SENSOR NETWORKS** under my supervision from December 2021 to March 2021.

Internal Guide:

Ms. YOGALAKSHMI.,ME.,(Ph.D)

Head of the Department:

Dr.T.RAVI,M.E.(Ph.D)

Submitted for Viva voce Examination held on

Internal Examiner

External Examiner

DECLARATION

I, SEELAM SUDHEER KUMAR REDDY (37130364) hereby declare that the Project Report entitled A NOVEL ANALYSIS OF HYBRID AND EFFICIENT INTRUSION DETECTION SYSTEMS IN WIRELESS SENSOR NETWORKS done by us under the guidance of MS. YOGALAKSHMI,M.E., (Ph.D) is submitted in partial fulfillment of the requirements for the award of Bachelor of Engineering degree in ELECTRONICS AND COMMUNICATION ENGINEERING.

DATE:

PLACE: CHENNAI

SEELAM SUDHEER KUMAR REDDY (37130364)

SIGNATURE OF THE CANDIDATE

ACKNOWLEDGEMENT

I am pleased to acknowledge my sincere thanks to Board of Management of **SATHYABAMA** for their kind encouragement in doing this project and for completing it successfully. I am grateful to them.

I convey my thanks to **Dr.N. M. NANDITHA, M.E., Ph.D.**, Dean, School of Electrical and Electronics and **Dr. T. RAVI, M.E., Ph.D.** Head of the Department, Dept. of Electronics and Communication Engineering for providing me necessary support and details at the right time during the progressive reviews.

I would like to express my sincere and deep sense of gratitude to my Project Guide **MS. YOGALAKSHMI, M.E., (Ph.D)** Assistant Professor for her valuable guidance, suggestions and constant encouragement paved way for the successful completion of my project work.

I wish to express my thanks to all Teaching and Non-teaching staff members of the **Department of Electronics and Communication Engineering** who were helpful in many ways for the completion of the project.

ABSTRACT

Wireless Sensor Networks (WSNs) have emerged as a promising technology due to their wide range of applications in industrial, environmental, military, and civil fields. Due to economic considerations, the nodes are usually simple and low-cost. However, they are often left unattended and may therefore be vulnerable to a variety of new attacks.

Wireless sensor networks (WSNs) have been increasingly deployed in applications that are responsive to protection. They are vulnerable to various security atrocities, and a black hole attack is a type of assault which, due to its resources, seriously affects data collection.

The most effective way to book the trip is to speak with an agent. According to the Media Richness Theory (Trevino et al., 1990), different media are capable of transmitting multiple signals, feedback immediacy, the use of natural language, and personal emphasis on the medium. Since there are no immediate website links or inputs, this is classified as a limited medium (Jarvelainen, 2003). Shim et al. (2001) contend that consumers use their knowledge in information collection. Theory of media suitability Their creativity, expertise, and ease of use are increasingly reinforcing the screen, emails, and other similar media.

Table of Contents

Page No.

BONAFIDE
CERTIFICATE.

DECLARATION.

ACKNOWLEDGEMENT.

ABSTRACT.

CHAPTER 1: INTRODUCTION

1.1 : WIRELESS NETWORKS

1.2 : OVERVIEW

ii

iii

iv

v

1

1

3

1.3: PLATFORMS

7

CHAPTER 2: LITERATURE REVIEW

8

2.1: A Structured Approach to Optimization of
Energy Harvesting Wireless Sensor Networks

8

2.2: Node Clustering in Wireless Sensor Networks:
Recent Developments and Deployment Challenges

9

2.3: Hierarchical routing in ad hoc mobile networks

11

2.4: Energy-Efficient Communication Protocol for
Wireless Micro sensor Networks

12

2.5: An Authenticated Trust and Reputation
Calculation and Management System for Cloud and
Sensor Networks Integration

14

CHAPTER 3 : RESEARCH METHODOLOGY

17

3.1 : EXISTING SYSTEM:

17

3.1.1 : DISADVANTAGES:

19

3.2 : PROPOSED SYSTEM:

19

3.3: SYSTEM ARCHITECTURE DISCRIPTION

21

3.3.1 : Data Flow Diagram

24

3.3.2: Activity Diagram

25

3.3.3: Use Case Diagram	26
3.4: MODULE DESCRIPTION	26
3.4.1 : Active Detection Routing	26
3.4.2: Nodal Trust	28
3.4.3: Data Routing	29
 CHAPTER 4 : SOFTWARE SPECIFICATION	 31
4.1: SYSTEM REQUIREMENTS	31
4.1.1 : HARDWARE REQUIREMENTS	31
4.1.2 : SOFTWARE REQUIREMENTS	31
4.1.3 : INDRODUCTION TO UBUNTU	31
4.2: IMPLEMENTATION TOOLS	32
4.2.1 : INTRODUCTION	32
4.2.2 : NS-2 LANGUAGE	41
4.2.3 : ARCHITECTURE OF NS-2	41
4.2.4 : MOTIVATION FOR SIMULATIONS	42
4.2.5 : NS FEATURES	42
4.2.6 : NS PROGRAMMING STRUCTURE	45
 CHAPTER 5 : RESULT AND DISCUSSION	 45
CHAPTER 6: CONCLUSION AND	51
FUTURE ENHANCEMENTS	53
 REFERENCE	 54

CHAPTER 1

INTRODUCTION

Wireless sensor networks (WSNs) are increasingly being deployed in security critical applications. Because of their inherent resource-constrained characteristics, they are prone to various security attacks, and a black hole attack is a type of attack that seriously affects data collection. The adversary compromises a node and drops all packets that are routed via this node, resulting in sensitive data being discarded or unable to be forwarded to the sink. Because the network makes decisions depending on the nodes' sensed data, the consequence is that the network will completely fail and, more seriously, make incorrect decisions. Therefore, how to detect and avoid BLA is of great significance for security in WSNs. There is much research on black hole attacks. Such studies mainly focus on the strategy of avoiding black holes. Another approach does not require black hole information in advance. In this approach, the packet is divided into M shares, which are sent to the sink via different routes (multi-path), but the packet can be resumed with T shares ($T \leq M$). However, a deficiency is that the sink may receive more than the required T shares, thus leading to high energy consumption; such research can be seen in [1]. Another preferred strategy that can improve route success probability is the trust route strategy. There is much related research, such as [2]. The main feature is to create a route by selecting nodes with high trust because such nodes have a higher probability of routing successfully; thus, routes created in this manner can forward data to the sink with a higher success probability.

1.1 WIRELESS NETWORKS

In Wireless networks use some sort of radio frequencies in air to transmit and receive data instead of using some physical cables. The most admiring fact in these networks is that it eliminates the need for laying out expensive cables and maintenance costs. Setting up a wireless system is easy and fast and it eliminates the need for pulling out the cables through walls and ceilings. Network can be extended to places which cannot be wired. Wireless networks offer more flexibility and adapt easily to changes in the

configurations of the network. Mobile users especially for Smartphone users are provided with access to real-time information even when they are away from their home or office. WSN is an infrastructure-less self-forming and self-healing network used for voice and data range extension in mission critical applications. The Cognitive and Software Defined Radio is a new paradigm for ubiquitous connectivity in tactical radios. The current research work is mostly focused to incorporate WSN s over wideband data waveforms. Most of the tactical radios deployed in the field are HF, VHF or UHF. Moreover, the next generation SDR will also support all the tactical waveforms. In our research work we proposed a secure cognitive device (SCND) for vehicular and tactical communication. The cognitive communication device seamlessly integrates HF, VHF, UHF, 802.11 radios based mobile ad hoc network with GSM, CDMA, WiMAX and Satellite networks.

Mobile Ad hoc networks are the basic building blocks to establish ubiquitous connectivity among mobile and fixed nodes in a geographical area. The nodes can either form local WSN or establish connection with the backbone to communicate with other MANETs, over longer distances. The mobile nodes operate in a wireless environment where multiple media covers patches of specified areas. The applications like NCW and IVN pose great research challenges to interconnect multiple networking technologies for extended coverage.

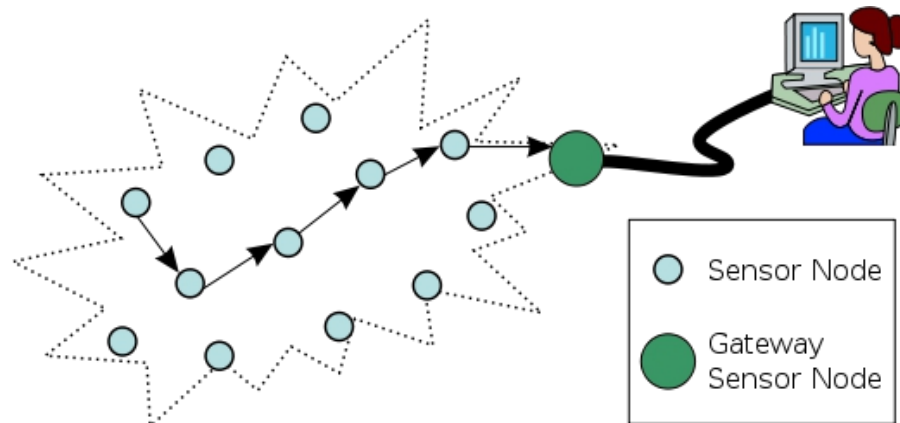
A Smartphone (or smart phone) is a mobile phone with more advanced computing capability and connectivity than basic feature phones. Smartphone's typically include the features of a phone with those of another popular consumer device, such as a personal digital assistant, a media player, a digital camera, and/or a GPS navigation unit. Later Smartphone's include all of those plus the features of a touch screen computer, including web browsing, Wi-Fi, 3rd-party apps, motion sensor, mobile payment and 3G. Smartphone is a Computer

Telephony Integration (CTI) product. This means it links your desktop computer and telephone system together. CTI is at the heart of the future office, and Smartphone was one of the first CTI products of its kind to be released in the United Kingdom. Smartphone belongs to a family of CTI

applications produced by Oak Telecom. Other parts of the family are Smart Connect and Smart Operator.

1.2 OVERVIEW

A wireless sensor network (WSN) consists of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring. The WSN is built of "nodes" – from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. Each such sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting. A sensor node might vary in size from that of a shoebox down to the size of a grain of dust, although functioning "motes" of genuine microscopic dimensions have yet to be created. The cost of sensor nodes is similarly variable, ranging from a few to hundreds of dollars, depending on the complexity of the individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and communications bandwidth. The topology of the WSNs can vary from a simple star network to an advanced multi-hop wireless mesh network. The propagation technique between the hops of the network can be routing or flooding.



APPLICATIONS

- Process Management
- Health care monitoring
- Environmental/Earth sensing
- Air pollution monitoring
- Forest fire detection
- Landslide detection
- Water quality monitoring
- Natural disaster prevention
- Industrial monitoring
- Machine health monitoring

CHARACTERISTICS

The main characteristics of a MANET include:

Power consumption constraints for nodes using batteries or energy harvesting

Ability to cope with node failures (resilience)

Mobility of nodes

Heterogeneity of nodes

Scalability to large scale of deployment

Ability to withstand harsh environmental conditions

Ease of use

Cross-layer design

Cross-layer is becoming an important studying area for wireless communications. In addition, the traditional layered approach presents three main problems:

Traditional layered approach cannot share different information among different layers which leads to each layer not having complete information. The traditional layered approach cannot guarantee the optimization of the entire network.

The traditional layered approach does not have the ability to adapt to the environmental change.

The standard layered approach for wired networks is not applicable to wireless sensor networks due to interference between users, access confliction, fading, and changes in the environment.

One of the primary goals of many WSN surveillance applications is to monitor a mobile target (such as a person or a vehicle). A target tracking system is also needed to ensure continuous monitoring, i.e., there are always nodes that can detect the target along its course, as opposed to detection, which studies discrete detection events (e.g., with low detection delay or high coverage level).

As a result, the most rigorous objective tracking requirement is to monitor with zero detection delay or 100% coverage. Since nodes are frequently powered by batteries that are difficult to recharge once deployed, energy efficiency is a critical feature of WSNs for extending network lifetime. However, improving energy efficiency would almost certainly have a negative impact on goal monitoring quality of service (QoS). Forcing nodes to sleep, for example, can result in the passing goal being missed and the tracking coverage being reduced. As a result, energyefficient target monitoring should boost the tradeoff between energy efficiency and tracking performance—for example, by increasing energy efficiency at the cost of a minor reduction in tracking performance.

Idle listening is a significant source of energy waste in target tracking applications. Duty cycling is one of the most widely used methods for

reducing energy usage during idle listening. The concept behind duty cycling is to put nodes to sleep for the majority of the time and then wake them up when necessary. In certain cases, nodes' sleep patterns can be deliberately scheduled, i.e., they can be compelled to sleep or awakened on demand. This is often referred to as sleep management. Proactive wake-up has been studied as a compensation for monitoring performance loss caused by duty cycling and sleep scheduling, with the aim of waking nodes proactively to plan for the approaching deadline. Most constructive wake-up attempts, on the other hand, literally wake up all neighbor nodes in the region where the target is supposed to arrive, with no distinction. In reality, waking up all of your neighbors isn't always important. To specifically sleep-schedule nodes in order to minimize energy consumption during proactive wake-up. If nodes know a target's exact path, for example, it will suffice to wake up those nodes that cover the route during the period when the target is supposed to pass through their sensing areas. Wireless sensor networks (WSNs) are commonly used in environmental monitoring, sensing, and data collection. The problem of locating target nodes in wireless sensor networks is a fundamental one. The most popular WSN localization algorithms can currently be divided into two categories: rangebased and range-free. In order to estimate position, range-based algorithms use distance or angle estimates. Connectivity information between unknown nodes and anchor nodes is used in range-free algorithms. Range-based localization algorithms must first determine the exact distances or orientations between adjacent nodes, then use that information to locate unknown nodes. In functional localization systems, measurement errors will occur, resulting in noisy range estimations. As a result, range measurements have a significant impact on location estimation accuracy. The accuracy of the current range-based algorithms cannot be improved without improving range estimation or adding any other information related to localization. For several years, indoor WSN localization has been a hot research subject. It is very difficult to locate an indoor mobile target due to the randomness of targets moving and the complicated indoor climate.

1.3 PLATFORMS

HARDWARE—Producing low-cost and small sensor nodes is a major challenge in a WSN. WSN hardware is being produced by a growing number of small businesses, and the commercial situation is comparable to home computing in the 1970s. Many of the nodes, especially their software, are still in the research and development stage. The use of very low power radio communication and data acquisition methods is also a function of sensor network adoption. A gateway connects a WSN to a Local Area Network or a Wide Area Network in many applications. The Gateway serves as a connection point between the MANET and other networks. This allows data to be stored and processed on computers with more power, such as a server that is located remotely.

SOFTWARE—Energy is the most scarce resource available to WSN nodes, and it decides the WSN's lifespan. WSNs can be deployed in large numbers in a variety of settings, including remote and hostile areas, where ad hoc communication is essential. As a result, algorithms and protocols must deal with the following issues:

Maximizing your life expectancy: Power/Energy Since their limited energy supply dictates their lifetime, the sensing device's consumption should be reduced and sensor nodes should be energy efficient. When the radio transceiver is not in use, the nodes usually switch it off to save power.

CHAPTER 2

LITERATURE REVIEW

2.1. A Structured Approach to Optimization of Energy Harvesting Wireless Sensor Networks

Fading channels can be used to evaluate the data maximisation problem for energy collection wireless sensor networks. The efficient application of energy collection networks for wireless sensors necessitates a thorough understanding of the underlying environmental processes. To maintain good performance over time, energy must be used as a limited resource, with sensor performance and power consumption traded off. We create a power-allocation algorithm based on sensor and time observations of the underlying structure of the optimization problem. We examine the problem's basic characteristics and present an overall energy flow limit sum rate algorithm that is optimal given the available energy and fading coefficients. We present simulation results to validate the theory and algorithm. In order to save resources, the node service period should be as short as possible. As a result, the nodes go through a brief wake cycle after a long sleep. The target is not found while a node sleeps, resulting in a blind detection period. This program's detection frequency in a perceived interval is 1. The Sensing Frequency One (TDSFO) target detection system is what we call it. To increase target monitoring performance, a new intelligent solution called the Sensing Frequency K Target Detection (TDSFK) system is proposed. The TDSFK's main idea is to split the sensing task loop into small chunks when nodes are up, so they aren't sleeping. The objective identification becomes more accurate as a result of this. The TDSFK scheme must, however, account for the energy used in state transformation, which has been overlooked in previous studies. The authors discovered that the state shift needed some energy from the processors and sensors. They also stated that the mote sensor Mica requires 4m to start. As a result, optimizing the given node sensing frequency to improve life and track efficiency is a significant research issue. In this paper, we propose an intelligent adjustable sensing frequency for mobile target detection based on display quality optimization. TDASF and TDSFK are two systems that have been proposed. The first

scheme makes use of the network's residual energy benefits to improve the performance of the display by using the unequal frequency of sensing in different areas. The formula for calculating the correct frequency value calculation is given by the second system. Three criteria were used to evaluate the proposed schemes' performance: missed goal chance, delay, and life time. The TDASF software will increase network life by more than 17.4% and reduce weighted detection delays by more than 101.6 percent, according to the results of the computer simulation. The algorithm for static WSN sinks, which are not suitable for cellular discharge networks, is presented in this paper. As a result, we'll continue to look into the target detection optimisation problem in the mobile device network.

2.2 Node Clustering in Wireless Sensor Networks: Recent Developments and Deployment Challenges

The large-scale implementation of wireless sensor networks (WSNs) and the need for data aggregation necessitate efficient network topology organization for load balancing and network lifetime extension. Clustering has been shown to be a good way to organize a network into a linked hierarchy. In this article, we address the difficulties of clustering a WSN, discuss the design justification for various clustering approaches, and identify the proposed approaches according to their goals and design principles. We also go through a few main issues that have an impact on the realistic implementation of clustering techniques in sensor network applications.

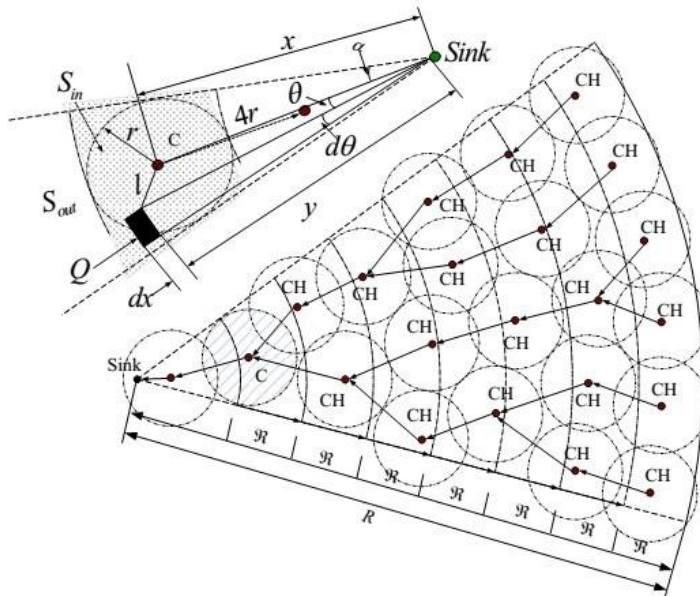
With the multi-NACK mechanism, energy for data collection in intra-cluster is conserved, and transport delay is reduced. In the meantime, if a sensor node sends some data packet, multi-ACK is returned in inter clusters. Despite the fact that the number of ACKs to be sent has increased, the number of data packets to be retransmitted has decreased significantly, lowering node energy consumption. The BCMN/A protocol is tested using both theoretical research and detailed simulations, and the results show that our proposed protocol optimizes both network lifetime and transport delay while maintaining network reliability.

We investigate the node energy consumption and transport delay in cluster-based networks under various reliability conditions. According to the results of the theoretical study, there is an ideal cluster radius for maximizing

network lifetime and minimizing transport latency. However, the cluster radius value that achieves maximum lifetime and minimal delay is not always the same.

Broadcasting Combined with Multi-NACK/ACK (BCMNA, where NACK stands for "Negative-Acknowledgment" and ACK stands for "Acknowledgment") is a novel data collection protocol that optimizes both energy and delay performance under statistically reliable constraints.

Extensive modeling studies are carried out by us. Simulation results back up our theoretical findings, demonstrating that the BCMNA protocol is efficient in terms of both energy and latency under network reliability constraints, improving network lifetime by 8% and reducing transport delay by 25% on average.



2.3. Hierarchical routing in ad hoc mobile networks

Clustering is a mechanism in which nodes are grouped hierarchically based on their proximity to one another. To improve routing flexibility, the routes through clusters can be recorded hierarchically. By improving road robustness, hierarchical routing greatly enhances routing scalability within ad hoc networks. It defines a cluster hierarchy of cluster leads and gateways to interconnect clusters using a protocol. The Adaptive Cluster Route is defined in this article (ARC). ARC uses a new algorithm for revocation of the cluster leader that eliminates the rip impact of leadership changes. ARC employs a minimal broadcast algorithm to mitigate the effects of network flutters. This is referred to as the energy supply dilemma. Based on practical wireless

recharging models and experimental results, we investigate two types of problems: point provision and road supply. The point provisioning uses the fewest number of readers in order to provide a sufficient re-charge rate for sustained operation to static tags placed in the network. The route provision takes advantage of tags' potential flexibility (for example, tags worn by humans) to further reduce the number of readers required: mobile tags can harvest excess energy in powerful regions and store it for later use in power-deficient regions. Our research has shown that by using the physical characteristics of wireless charging, we can significantly reduce the number of readers as compared to traditional coverage models. Above, we discussed two forms of energy supply issues: 1) the provision of points; 2) the provision of paths. In point provisioning, the WISP tags are meant to be static. Regardless of where a tag is placed on the network, readers must ensure that their recharging rate (i.e. collected electricity per second) is no less than the mean energy consumption (i.e., energy consumed per second). WISP tags are expected to switch when they're used by humans or when they're attached to other mobile entities, such as in route provisioning. In this case, even though a tag can only produce energy at a low rate along a portion of its path, it can still be sustainable if it can harvest enough additional energy along the path and has a large enough condenser to store the extra electricity.

The aim of path supply is to determine how to deploy readers based on the mark's mobility pattern so that the median charge rate over time is high enough. Because of the distance between the tag and the reader, a function of the energy obtained by the second, the wireless model of a WISP tag must first be understood in order to solve the above two types of supply in WRSN's. A practical charging model is proposed, based on Friis' well-known free space equation, and extensive experimental data is used to fit the parameters. The charging model is based on the reader's distance from the device. The charging power corresponds to the average WISP tag energy consumption, so r_1 is the distance threshold. If the tag is more than 1 meter away, To ensure tag delivery, multiple readers can be used from any reader. As a result, another issue is how many competing readers would have an effect on wireless recharge. The wireless charging model is additional,

according to experimental results, since the combined charging power of multiple readers is equal to the amount of charging power of each reader. We'll also look at the effects of mobility on charging, using experimental data from WISP mobility tags, to prove that mobility can be beneficial. variable is smoothed out Impact of radio waves on a small scale due to environmental factors.

2.4. Energy-Efficient Communication Protocol for Wireless Micro sensor Networks

For both civil and military applications, wireless distributed micro sensor systems will allow accurate monitoring of a variety of environments. The communication protocols examined in this paper can have a substantial effect on the total energy dissipation of these networks. We propose LEACH (Low-Energy Adaptive Clustering Hierarchy), a clustering-based protocol that uses randomized rotation of local cluster base stations (cluster-heads) to evenly distribute the energy load among sensor networks, based on our findings that the conventional protocols of direct transmission, minimum-transmission-energy, multi-hop routing, and static clustering may not be optimal for sensor networks. LEACH integrates data fusion into the routing protocol to minimize the amount of data that must be transmitted to the base station and uses localized coordination to allow scalability and robustness for complex networks. The adopted scheme model is identical to this article. To show, we use a cyber-physical device (CPS). The device is made up of three parts: (a) Users, or consumers. Users may access services by making the required payment to SOs. (b) Service Operators (SOs) collect basic (SS) services from businesses and then terminate them by delivering more informative and better services to customers. Organizations that provide simple programs must be charged in equivalent amounts at the same time. N CPS bodies, N CPS bodies, N CPS bodies, N CPS bodies, N CPS bodies, N C From the source, companies collect essential resources in the CPS. SOs are in charge of all services. The vast majority of businesses obtain primitive basic services (SS) by sensing the environment. To collect SS and accept payments from SS to SOs, a company must pay a certain amount. Furthermore, SS or interactions between companies can benefit businesses (game). The market competition between the buyer and SOS has been

extensively studied. The emphasis of this paper is on the more competitive price competition between SOS and the company, as well as between companies.



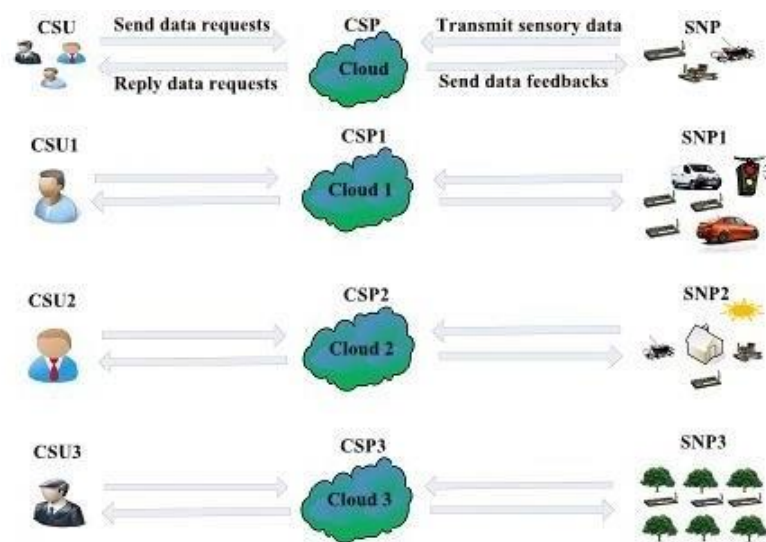
The main goal of SOS is to provide users with more comprehensive and improved services. However, in order to collect such basic resources, SOS publish certain service gathering tasks to the application's area of interest (AOI). For example, traffic information collection can be considered a simple service gathering activity. Entities in the AOI obtaining the service gathering task decide whether or not to take part in the task. If an organization wishes to perform service gathering, it will collect services, send them to SOS, and receive payoffs based on the service price set by the SOS. Finally, the SOS make their available composite services available to consumers and receive payment from them. It's the same in CPSs; we only consider one service application that necessitates continuous service collection (traffic jams, environmental monitoring and security such as noise, smog/haze detection, citizen journalism, tourist queries, and so on).

2.5. An Authenticated Trust and Reputation Calculation and Management System for Cloud and Sensor Networks Integration

The CC-WSN integration has gained a great deal of attention from both academia and the industry, due to the incorporation of the strong data storage and data processing skills of Cloud Computing (CC) as well as the ubiquity of data collection of WLANs. The authentication and measurement of confidence and credibility and administration of Cloud Service Providers (CSPs) and SNPs are two extremely important and scarcely discussed problems. This paper proposes an authenticated new method for CC-WSN

integration, namely confidence and credibility measurement and management (ATRCM). Taking into account the authenticity of CPS and SNP, the Cloud service user (CSU) and CSP attributes, the costs, trust and reputation that CSP and SNP service requires, the proposed ATRCM system performs the following three functions: 1) the ability to authenticate CSP and SNP in order to prevent malicious impersonation attacks; 2). In order to show the efficacy of ATRCM and to follow up with system-security analytics detailed analysis and design and further functionality evaluation results are discussed.

In this paper, as the key of our work is to enable CSU to choose the authentic and desirable CSP as well as assist CSP in selecting genuine and appropriate SNP, we focus on the authentication of CSP and SNP rather than the authentication of CSU. Specifically, the CSP needs to prove its authenticity to CSU and SNP has to show its authenticity to CSP. Here, ISO/IEC 27001 certification [33], [34] is applied to authenticate CSP and SNP, as it is an internationally recognized information security management system (ISMS) standard by the International Organization for Standardization (ISO) and the International Electro technical Commission (IEC). It requires that the information management of an organization (e.g., CSP or SNP) meets (i) the organization's information security risks are systematically examined; (ii) a coherent and comprehensive suite of information security controls is designed and implemented to solve those risks that are deemed unacceptable; (iii) an overarching management process is adopted to ensure that the information security controls continue to satisfy the organization's information security needs on an ongoing basis. Particularly, it provides confidence and assurance to trading clients of the organization, as the security status of the organization is audited to be qualified, by issuing a certificate with the ISO/IEC 27001 certification. After CSP and SNP are certificated with ISO/IEC 27001, they obtain the certificates (i.e.,ctc and ctk) respectively.



In addition, our system security analysis powered by three adversary models showed that our proposed system is secure versus main attacks on a trust and reputation management system, such as good mouthing, bad mouthing, collusion and white-washing attacks, which are the most important attacks in our case.

While several node implementation techniques are proposed, their general aim is only to balance energy consumption overall. However, a guaranteed network T lifetime, which has not been considered in previous research is normally required in mission-critical applications. We therefore see a more realistic situation in which the deployment strategy of the node deals with how the few sensors to ensure the necessary network life time T are deployed. In order that we can achieve optimum network performance when the network lifetime per unit implementation is the biggest. The ultimate aim of the node implementation strategy is to ensure a minimum of sensors for T network existence. Thus the node deployment approach in this paper, used as an optimization metric for network performance, best meets WSN's actual requirement.

CHAPTER 3

RESEARCH METHODOLOGY

3.1 EXISTING SYSTEM:

A collaborative anomaly detection system combines the already existing structure with lightweight authentications, that correlates the alerts of lightweight IDSs across the WSN. SDN's resource-restricted data plane lightweight authentication system requires a software-defined, software-based, wireless sensor networking authentication system (IPS) (SDWSNs). This system protects the network by permitting authenticated nodes to insert only correct information. The authentication of the nodes must also be carried out constantly and often, raising its complexity significantly. Moreover, an authentication system based on IPS may be implemented through one or more validation elements like credentials, factors of information (interchange keys), factors of possession (token) and biometrical factors (eg., fingerprint recognition, iris, face, retina, etc.). Though validation factors can be a low-latency solution, they also add difficulty because of repeated authentication transfers. However, the standard IPS authentication procedures depend on encryption keys and numerous handshakes, such as AKA protocols.

However, they were found to be unsuitable for the requirements of SDWSN due to their high latency, low transfer rates and high computational costs. Though malicious nodes can effectively be identified by IPS-based authentication methods, they cannot remove everything, in particular those started from the Internet. Furthermore, the captured nodes have full control over encryption and authentication key assets and can easily launch attacks. Therefore mobile nodes are likely to be hacked, abused and hidden without additional security. IDS-based solutions will include a second invaluable line of protection in order to ensure the data plane is protected from insider attacks in SDWSNs. Machine learning processes like SVM and neural networks are commonly used to this purpose. Such methods, however, usually introduce a high computational costs and overheads in SDWNs which are not negligible. Models for energy prediction centered on edge may be used to minimize the overhead introduced by machine learning solutions.

The sensor nodes are, however, individually susceptible to a huge number of warnings. A warning does not always imply problems, but it may simply be an indication that a traffic which matches a signature or a pattern has been inspected by the sensor. This makes the malicious and reliable operation an anomaly. These warnings are referred to as false positive and can subvert a sensor network. The reason is that the sensor nodes have local network activity visibility only. The shopbased existence of power characteristics in wireless communication, on the other hand, can lead to an IDS-enabled power prediction model.

Therefore, the use of a real-time Smart Monitoring System (SMS) using a control-level machine-learning algorithm is an encouraging solution to eliminate false alarms and to improve the decision making process by combining the decisions that an IDS already takes. Because the proposed SMS is installed on the control plane, it can be tailored to the particular topology and network operator requirements/issues with additional security services. This work therefore proposes a collaborative software-defined safety system to organize various controls of protection on each frame layer rather than independent security schemes. The criticality of the wireless system, its security requirements and its resource constraints are the basis for each security control. The work proposes a collaborative system design for security with the aim of achieving high safety, tackling limited resources and using SDN architectures. In short, there is a hierarchy and three levels of the proposed security architecture. At the bottom of the stack, an IPS authentication procedure is carried out on the data plane in L1. In the centre, at the border, in L2, there is an IDS model for energy prediction, and the SMS SVM algorithm is built in the control plane, in L3. In this sense, a clusterbased WSN is generated in L1, and DSA is used to start the acquisition process with sink nodes by sending a sign to their cluster heads, thus forging a global energy status. The marker message would then be sent to the members of the cluster. Each member returns their energy state to their cluster head post to receive the message. Using an embedded watermarking tool, the Head of the Cluster collection of the globalized energy state from their members ensures that the data extracted are not altered by any potential malicious attackers on the fly, by the use of a public key created

and other security parameters. The network snapshot and the watermarked data are then transmitted to the sink node. Also, the sink sends to the control level in the cloud a copy of the energy diagram. In addition, in order to ensure continuous authentication and subsequent energy consumption forecasting, periodically a sink node is received by the snapshot readings in order to recognize the embedded watermark. In addition, the relevant watermarked information is considered reliable while the data are marked as inaccurate, without a proper watermark. Subsequently, in L2, an IDS model for energy forecasting is executed, which uses a protocol for the Markov chain prediction to detect misbehavior of nodes. To finish, an SMS-based SVM algorithm is designed to amalgamate this system in the L3 control plane, whereby an SVM classification algorithm is used to process the dataset resulting from L2.

3.1.1 DISADVANTAGES:

1. Network traffic occurs in this framework, it results in data loss.
2. Unused nodes are not calculated, which is most important during the data congestion.
3. Attacks like Eavesdropper will affect this framework, by gathering the data while communication between two nodes.

3.2 PROPOSED SYSTEM:

Due to their wide variety of applications in industry, environmental surveillance, military and civilian fields, wireless sensor network (WSN) are a promising technology. The nodes are typically easy and cheap because of economic considerations. However, they are often unattended and are thus likely to be affected by various new attacks.

Hybrid IDS has been designed to resolve SIDS and AIDS disadvantage by integrating SIDS and AIDS for unknown and identified attacks. We used AIDS in our approach to detect invisible intrusions and SIDS is used to identify known attacks. The three phases of our method are focused on. Our methods for intrusion detection include online and offline, meaning detection of later and online intrusions, meaning real-time intrusions. The network traffic will be analyzed in this stage to determine if it is an infringement.

3.3 SYSTEM ARCHITECTURE DISCRIPTION

In this paper, using recent advances in uncertain reasoning originated from artificial intelligence community. We propose a trust management scheme that enhances the security in networks name Hybrid and Efficient Intrusion Detection Systems (HEIDS). Here we used two frameworks for Trust Calculation and Decision Making process. The trust value is derived using Bayesian Inference, and Decision Making based on Dempster-Shafer theory, which is a mathematical theory of evidence.

The Trust scheme is the first routing scheme that uses active detection routing to address BLA. The most significant difference between Active Trust and previous research is that we create multiple detection routes in regions with residue energy; because the attacker is not aware of detection routes, it will attack these routes and, in so doing, be exposed. In this way, the attacker's behavior and location, as well as nodal trust, can be obtained and used to avoid black holes when processing real data routes. To the best of our knowledge, this is the first proposed active detection mechanism in WSNs. Improving energy efficiency is the Trust Road Protocol. In WSNs, energy is very valuable and if successful detection is processed, more energy will be consumed. Therefore the adoption of such high-energy-consumption active detection routes was unlikely in previous research. But after a thorough analysis of the energy consumption of WSNs we find it plausible. Research has shown that up to 90% of residual energy still exists in WSNs, when the network dies from the "energy hole" phenomenon. The Active Trust system therefore uses residual energy to establish routes of detection and attempts to reduce energy consumption in hotspots (to improve network lifetime). These detection routes can detect the nodal trust and thus increase network protection without decreasing lifetime. The

Active Trust system's energy efficiency is enhanced more than two times in comparison with previous routing systems, including the shortest routing, crosscutting, according to theoretical research and test results.

Increased safety efficiency of the trust scheme. In Active Trust, nodal confidence can be obtained compared to previous study. The path is based

on the theory that follows. To avoid possible attacks, select nodes with high confidence, and then proceed along a successful detection path. The above approach allows for better network security.

The Active Trust routing scheme proposed in the paper will increase the likelihood of a successful roadway by 1,5 times to 6 times and energy efficiency by more than 2 times as in earlier studies, through our comprehensive theoretical analysis and simulation review. (4)

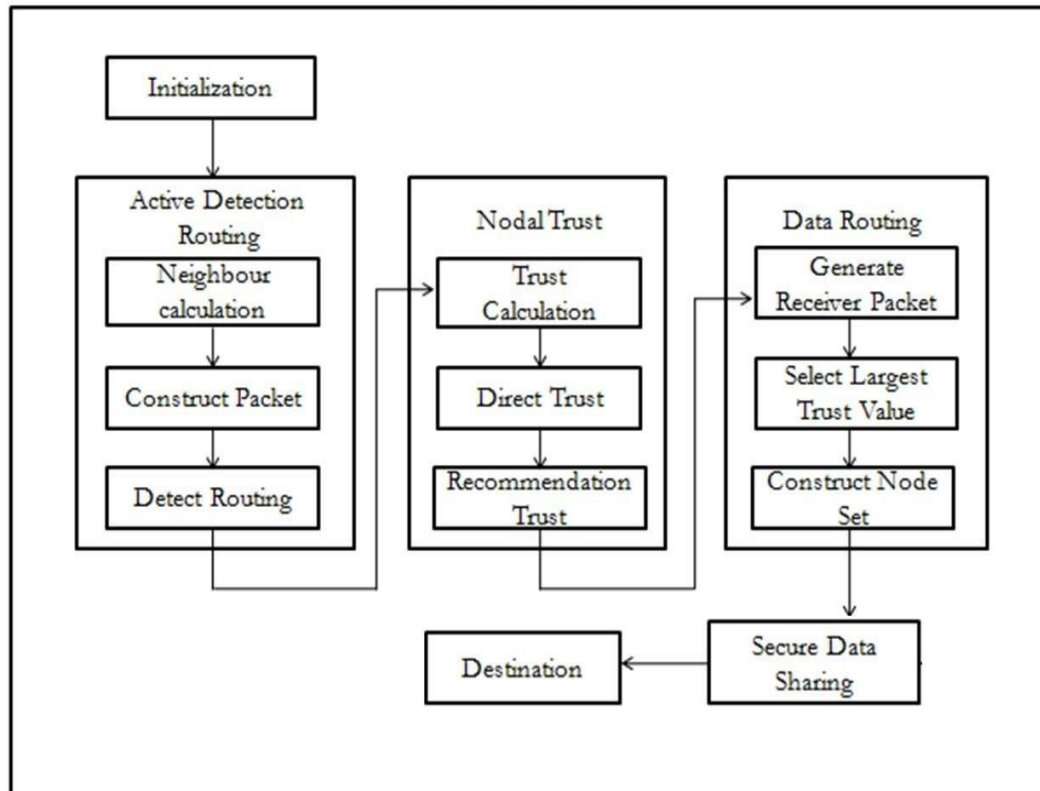
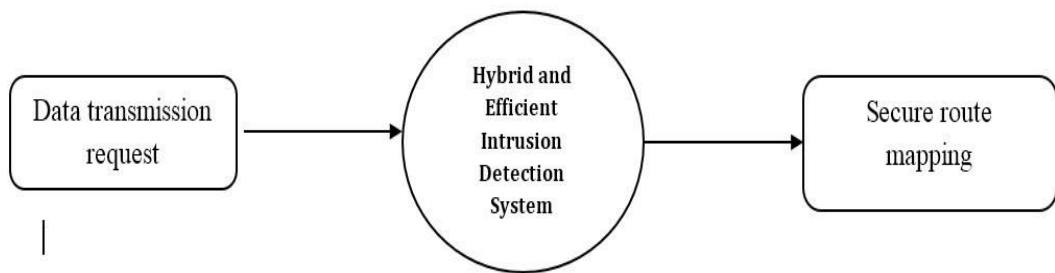


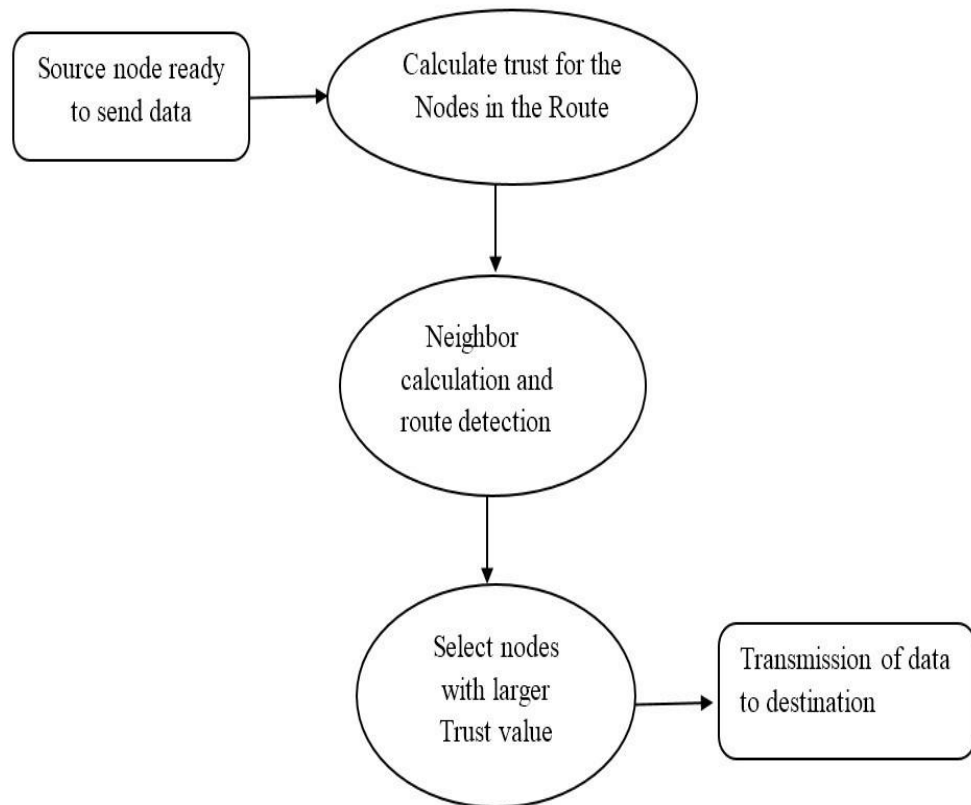
Fig 3.1 Proposed work Architecture

3.3.1 Data Flow Diagram

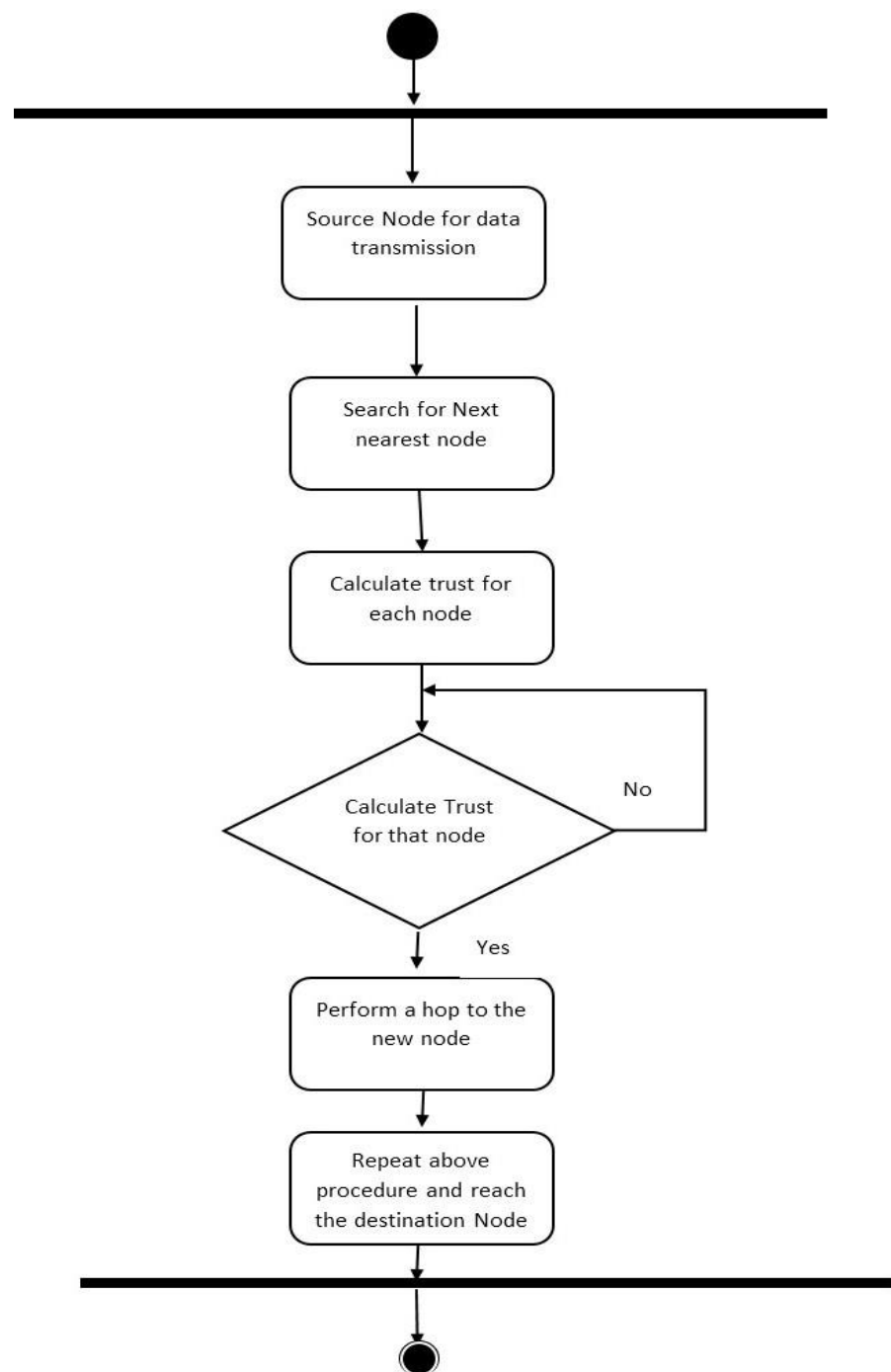
Level-0



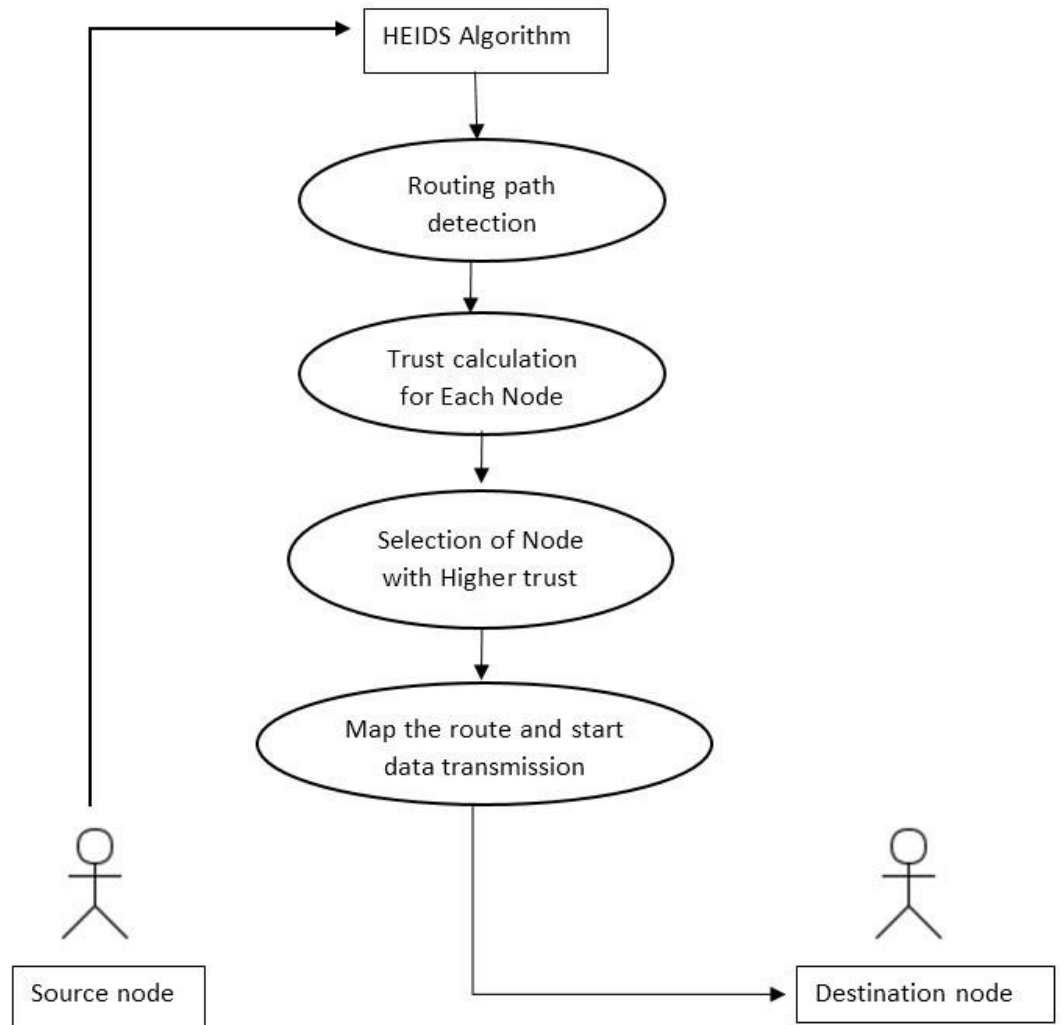
Level – 1



3.3.2 Activity Diagram



3.3.3 Use Case Diagram



3.4 MODULE DESCRIPTION

The architecture can be divided into three main modules.

- *Active Detection Routing*
- *Nodal Trust*
- *Data Routing*

3.4.1 Active Detection Routing

A track detects a path without data packings that is intended to convince the opponent to initiate an attack in order to define the action of the attack and then mark the position of the black hole. The system therefore reduces the trust of suspect nodes and increases the confidence of nodes in successful routes. Via active detection, nodal trust can be quickly gained and the data

route can be effectively selected to escape black troubles. The source node selects an undetected neighbor node at random in this scheme to establish an active detection path. In view of the fact that the longest detection route is w , the detection route reduces its duration by 1 per hop up to 0, which then ends. This section describes how the active detection routing protocol is implemented. As shown in Figure 2 the content can be divided into 6 sections of the detection routing packet: (b) the source node identification; (d) the maximum route length of the detection route; (e) the recognition that each of the wops is backed to the source; and (f) the packet identification.

head	type	source	w	w	id
------	------	--------	-----	-----	----

To start the detection process, the source node selects an undetected node. The overall route length is reduced by 1 until the detection packet receives nodes. If 0 is then generate a feedback packet, start a feedback path to the source and restore the initial value. If not 0, the next hop is selected as well; otherwise the path is terminated. The feedback package is structured and comprises six parts: (a) the header of a packet; (b) the type of packet; (c) the source node ID; (d) the destination node;

head	type	source	Destination	S-id	id
------	------	--------	-------------	------	----

The feedback packet is routed back to the data source; because nodes cache the detection route info, the feedback packet is able to return back to the source, and the following is the algorithm for the detection route protocol.

3.4.2 Nodal Trust

During data routing and detection routing, every node will perform a nodal trust calculation to aid in black hole avoidance. When node A performs a detection route for node B at time t , if the detection data are successfully routed.

$$\{\Delta_A^B(t_1) | \Lambda_A^B(t_1), \Delta_A^B(t_2) | \Lambda_A^B(t_2), \dots, \Delta_A^B(t_w) | \Lambda_A^B(t_w)\}$$

Then, during period t , the total direction trust of A to B is:

$$\begin{cases} C_A^B = \sum_{i=1}^w \{(\Delta_A^B(t_i) \mid \Lambda_A^B(t_i)) \cdot h(i)\} & w \neq 0 \\ 0 & w = 0 \end{cases}$$

Nodal direction trust: Consider the trust set of node A to node B during t to be:

Nodal recommendation trust: Node A is the trust evaluator, node C is the target of evaluation, and node B is a recommender of A. Consider $B \rightarrow A \rightarrow C$ to be the direction trust of A to B and $C \rightarrow B \rightarrow C$ to be the direction trust of B to C; then, the recommendation trust of A to C is

$$R_A^C = C_A^B \times C_B^C$$

For the trust of multiple recommendations, the calculation of the recommendation trust from A to B, B to C, etc., until D to E is

$$R_A^E = C_A^B \times C_B^C \times C_C^D \times C_D^E$$

Recommendation trust merging: Consider that the recommender set of node

A is AR , $n_i \in AR$ and that the recommendation trust of n_i to node K is $R_{n_i}^K$; then, the merged trust of A to K is

$$U_A^K = \sum_{n_i \in AR} (u_{n_i} R_{n_i}^K) \mid u_{n_i} = \frac{R_A^{n_i, K}}{(R_A^{n_1, K} + R_A^{n_2, K} + \dots + R_A^{n_{m-1}, K} + R_A^{n_m, K})}$$

Comprehensive trust: Comprehensive trust is the total trust, which merges the recommendation trust and direction trust:

The comprehensive trust of a node can be computed as follows. After the node launches a detection route, it calculates the direction trust according to Eq.

For each received feedback packet. Through interactions, the node obtains the recommendation trust from its neighbors according to Eq. (1), and it then calculates the merged trust according to Eq. (2), for the multiple-recommendation trust. Finally, it calculates the comprehensive trust according to Eq. (3).

3.4.3 Data Routing

The data routing refers to the process of nodal data routing to the sink. The routing protocol is similar to common routing protocols in WSNs; the difference is that the route will select a node with high trust for the next hop to avoid black holes and thus improve the success ratio of reaching the sink.

The central principle of data routing is to pick a node from the group of applicants closer to the dish, whose faith is greater than the predefined threshold as the next hop when a data packet is received. If the node does not find such the right next hop node, the upper node receives a feedback failure, and the upper node recalculates the unselected node set and selects the node with the highest confidence as the second hop; likewise, when it can't find the next hop, the upper node will forward a feedback failure to the upper node. The top node, which works the same way, will pick another node from its neighbors near the platform before data is redirected to the platform or there is no way to the platform.

Algorithm 1: Active Detection Routing Protocol

```
1: Initialization
2: For each neighbor node  $A_n$  Do
3:   Let  $A_n.accessTime = Current\_time$ 
4: End for
5: For each node that generates a detection packet, such as node A, Do
6:   Construct packet P, and do value assignment for  $\omega$  and  $\overline{\omega}$ 
7:   Select B as the next hop which B meets access time is the minimum and
   nearer the sink
   //B is the node that is the longest time undetected and nearer the sink
8:   Send packet P to node B
9: End for
10: For each node that receives a detection packet, such as node B, Do
11:   let  $P.\omega = P.\omega - 1$ ,  $P.\overline{\omega} = P.\overline{\omega} - 1$ 
12:   If  $\overline{\omega} = 0$  then
13:     Construct feedback packet q, and do value assignment for each part
14:     Send feedback packet q to the source
15:   End if
16:   If  $P.\omega \neq 0$  then
17:     detection routing continue
18:   End if
19: End for
20: For each node that receives feedback packet q, such as node C, Do
21:   If q.destination is not itself then
22:     send q to the source node
23:   End if
24: End for
```

Algorithm 2: Data Routing Protocol

```
1: For each node that generates or receives a data packet, such as node A, Do
2:   select B as the next hop such that B has never been selected in this data
   routing process, has the largest trust and is nearer the sink
4:   If A finds such node, for instance, node B
5:     Send data packet P to node B
6:     If node B is the sink then
7:       this data routing procession is completed
8:     End if
9:   Else
10:    Send failure feedback to the upper node, such as node C
11:   End if
12:End for
13:For each node that receives failure feedback, such as node B, Do
14:  Repeat step 2 to step 11
15:End for
```

CHAPTER 4

SOFTWARE SPECIFICATION

4.1 SYSTEM REQUIREMENTS

4.1.1 HARDWARE REQUIREMENTS

❖ Processor	:	Intel Pentium IV
❖ Processor Speed	:	1.4 GHz
❖ Memory (RAM)	:	Default
❖ Hard disk	:	Default
❖ Monitor	:	Default
❖ Input Device	:	Keyboard (104)

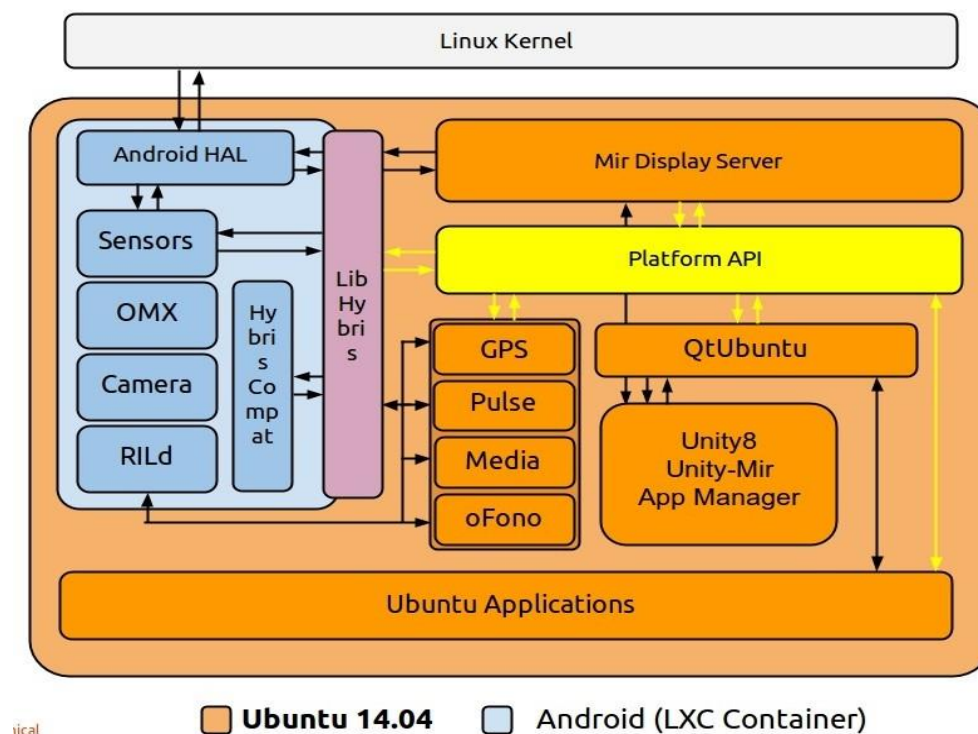
4.1.2 SOFTWARE REQUIREMENTS

❖ Operating System	:	Ubuntu 10.04
❖ Simulator Tool	:	NS 2.34
❖ Language	:	TCL

- ❖ Protocol Design : C++
- ❖ Platform : Independent

4.1.3 INTRODUCTION TO UBUNTU

Ubuntu is a Debian-based Linux operating system, with Unity as its default desktop environment. It is based on free software and named after the Southern African philosophy of Ubuntu (literally, "human-ness"), which often is translated as "humanity towards others" or "the belief in a universal bond of sharing that connects all humanity". According to some metrics, Ubuntu is the most popular Linux distribution.



4.1.3 Architecture Design Ubuntu

4. 1.2 BENEFITS OF UBUNTU ❖ Low cost

- ❖ Performance
- ❖ Flexibility
- ❖ Compatibility
- ❖ Choice
- ❖ Fast and easy installation
- ❖ Multitasking
- ❖ Security

- ❖ Open Source

4.1.3 TCL LANGUAGE

TCL (Tool Command Language) is a scripting language created by “John Ouster out”. Originally "born out of frustration", according to the author, with programmers devising their own languages intended to be embedded into applications, TCL gained acceptance on its own. It is commonly used for rapid prototyping, scripted applications, GUIs and testing. TCL is used on embedded systems platforms, both in its full form and in several other small-footprint versions.

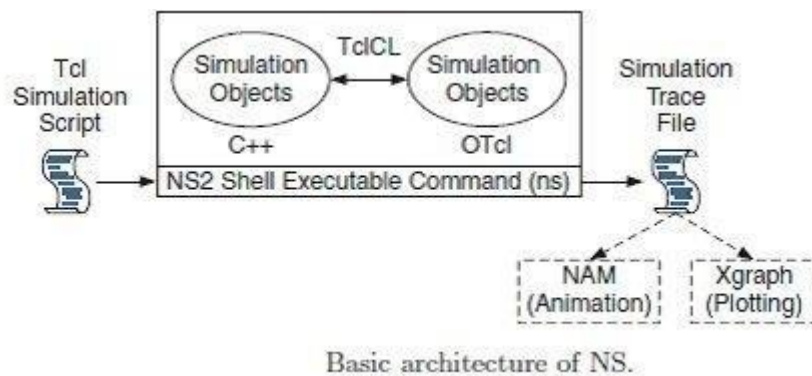


Figure 4.1.2 Tool Command language

The features of TCL are:

- ❖ Everything can be dynamically redefined and overridden.
- ❖ All data types can be manipulated as strings, including source code.
- ❖ Event-driven interface to sockets and files. Time-based and user-defined events are also possible.
- ❖ All commands defined by TCL itself generate error messages on incorrect usage.
- ❖ Extensibility, via C, C++, Java, and TCL
- ❖ Interpreted language using byte code
- ❖ Full Unicode support, first released 1999
- ❖ Cross-platform: Windows API, Unix, Linux, Macintosh, etc.
- ❖ Close integration with windowing (GUI) interface
- ❖ Multiple distribution mechanisms exist:

- ❖ Full development version (e.g., Active State TCL)

NS2 consists mainly of two languages. C++ and OTCL. Each of these two languages has its own strengths and weaknesses. NS2 beautifully integrates these two languages to draw out their strengths.

LINK

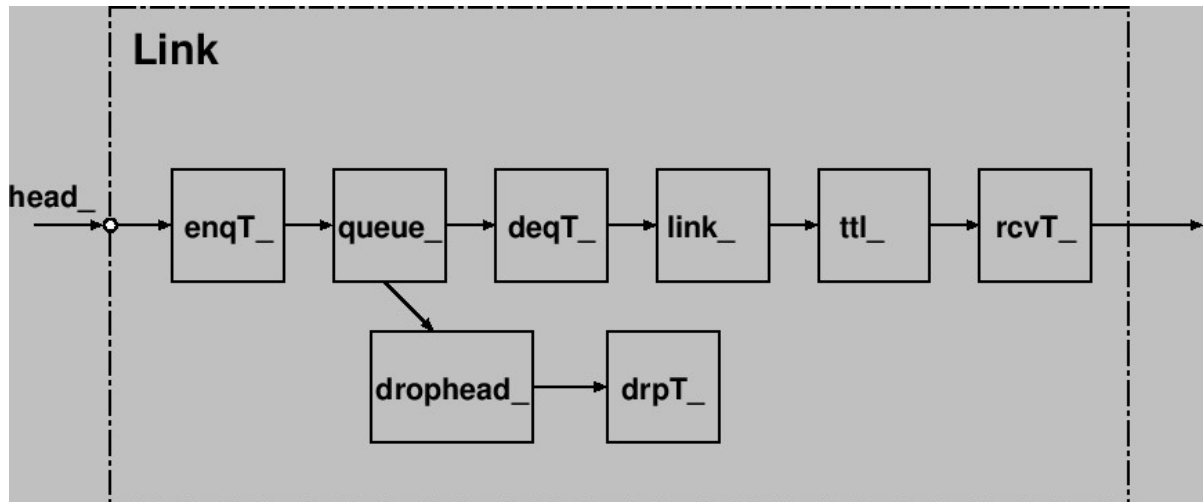


Figure 4.1.3 Link

Another important compound object in NS is a link. If a user creates a connection using a Simulator Object duplex link feature, two simple links are formed in both directions. One thing that needs to be noted is that a node output queue is actually used in a simple connection entity. Delay object which simulates the delay in links and packets dropped in queues are sent to a zero agent and freed there. Finally, for every packet received, the TTL object calculates the time to live parameters and updates the packet TTL area.

STARTING NS

NS starts with the command ns (assuming that we are in the directory with the ns executable, or that we have path points to that directory), where is the name of a TCL script file which defines the simulation scenario (i.e. the topology and the events).

We could also just start ns without any arguments and enter the TCL commands in the TCL shell, but that is definitely less comfortable. Everything else depends on the TCL script.

PROTOCOLS

Wireless networks have different routing protocols. DSR, AODV and DSDV are the most common. This study attempts to compare these three protocols in the

various environments on a performance basis. The NS2 is the main simulator, the NAM and Trace Graph used to make the plot from the trace files. The Simulation Tools are NS2. The results of the study clearly show that in different settings the various protocols act differently. The findings also highlight the essential features of various protocols based on their effectiveness and thus recommend improved protocols. Names of the protocol: WSN, AODV, D SR, DSDV, NS2.

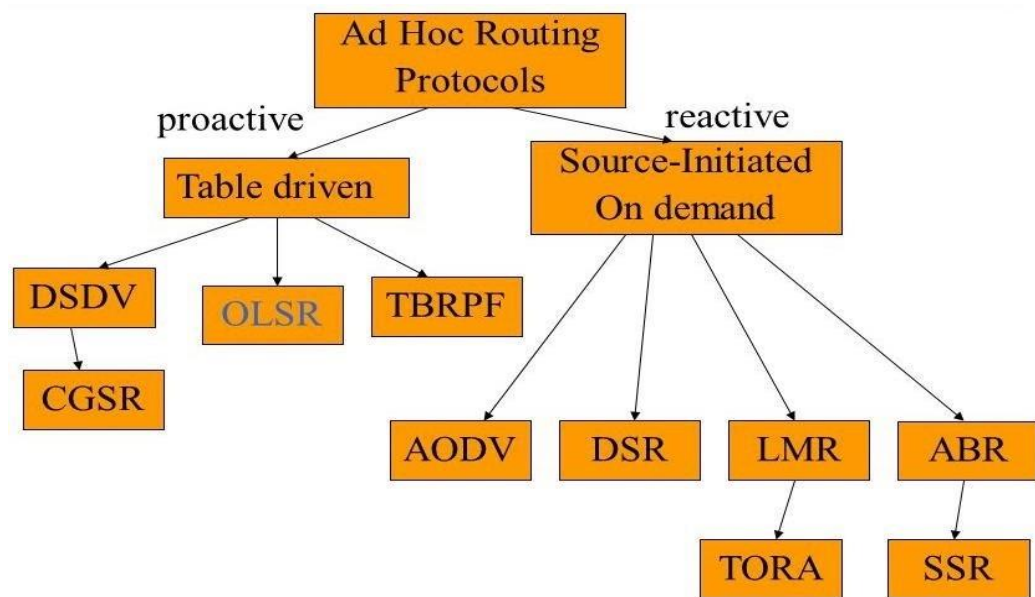


Figure4.1.4. Protocols

ROUTING ALGORITHMS

Most QoS routing algorithms represent an extension of existing classic besteffort routing algorithms. These algorithms can be classified into two different categories: on-demand (reactive) such as DSR, AODV, and TORA, and tabledriven (proactive) such as Destination Sequenced Distance Vector protocol (DSDV). In the on-demand protocols, routes are discovered between a source and a destination only when the need arises to send data. This provides a reduced overhead of communication and scalability.

DYNAMIC SOURCE ROUTING PROTOCOL (DSR)

DSR is one of the most popular ad hoc wireless network routing algorithms. It was built by Johnson, Maltz and Broch originally. DSR uses source routing that enables loop-free packet routing. The efficiency is increased by the use of promiscuous listening mode to cache routing information for future use, either through transmission of route discovery requests or by overhearing packets. The

routing protocol is easy and effective for ad-hoc networks. It is divided into two major stages: road detection and road maintenance.

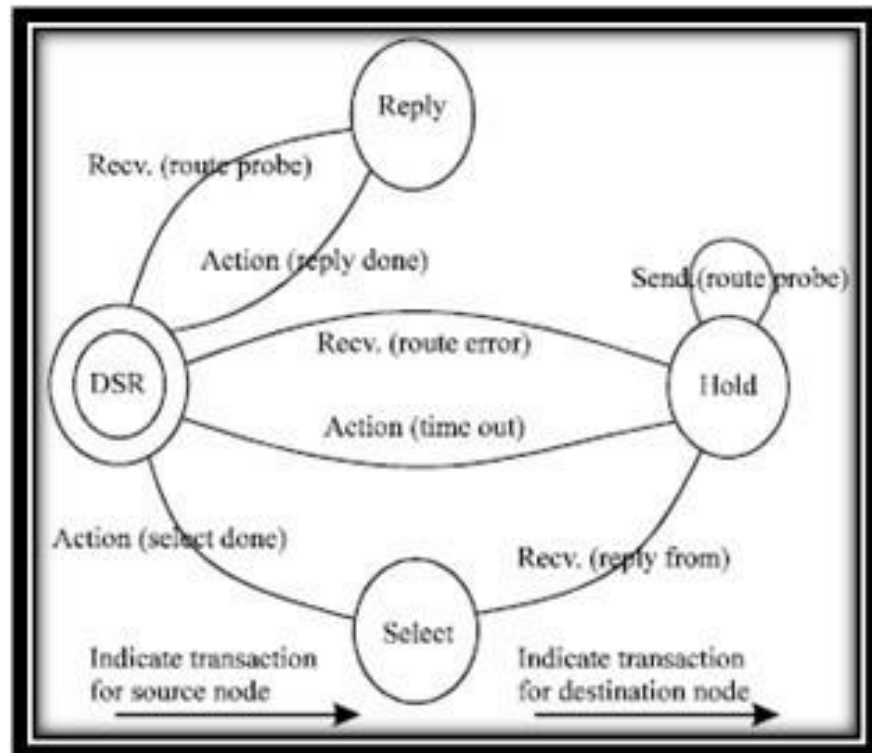


Figure 4.1.5 DSR Protocol

THE ADHOC ON DEMAND DISTANCE-VECTOR PROTOCOL

AODV is an additional ad-hoc network routing algorithm. In contrast to DSR, the source routing is not available, but is on-demand like DSR. In AODV the routing table used for storing destination and next hop IP addresses and destination sequence numbers is held in each node. The destination address of any entry in the routing table is next hop, the list of nodes of precursors, life and distance.

Interesting concepts of ADOV

Features

- ❖ Because of its reactive nature, AODV can handle highly dynamic behavior of Vehicle Ad-hoc networks.
- ❖ Used for both unicasts and multicasts using the 'J' (Join multicast group) flag in the packets.

Limitations

- ❖ Requirement on broadcast medium: The algorithm expects/requires that the nodes in the broadcast medium can detect each other's broadcasts.
- ❖ No reuse of routing info: AODV lacks an efficient route maintenance technique. The routing info is always obtained on demand, including for common case traffic.
- ❖ It is vulnerable to misuse: The messages can be misused for insider attacks including route disruption, route invasion, node isolation, and consumption.
- ❖ High route discovery latency: AODV is a reactive routing protocol. This means that AODV does not discover route until a flow is initiated.

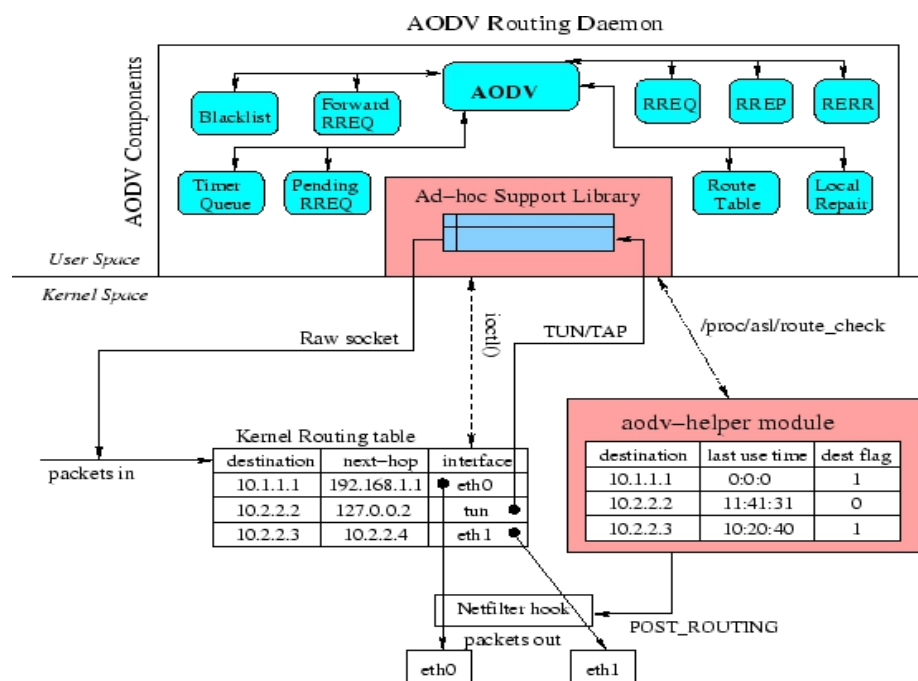


Figure 4.1.6 AODV Routing Protocol

DSDV - THE DESTINATION SEQUENCED DISTANCE VECTOR PROTOCOL

DSDV is one of the most popular routing algorithms for WSN table-driven systems. It's a protocol for the distance vector. The sequence of hops selected in this way leads to x along the shortest path. Each node tracks the cost of its outgoing links and regularly transmits its current estimate of its shortest distance to every other node in the network for the purpose of keeping distance forecasts up-to-date.

Advantages

- ❖ Count to infinity problem is reduced in DSDV. We can avoid extra traffic with incremental updates instead of full dump updates.

- ❖ Path Selection: DSDV maintains only the best path instead of maintaining multiple paths to every destination.

THE ADVANTAGES OF NETWORKING

Networks allow computers, and hence their users, to be connected together. They also allow for the easy sharing of information and resources, and cooperation between the devices in other ways. Some of the major benefits as follows.

- ❖ Connectivity and Communication

Networks connect computers and the users of those computers. Individuals within a building or work group can be connected into LAN.

- ❖ Data Sharing

One of the most important uses of networking is to allow the sharing of data. True networking allows thousands of employees to share data much more easily and quickly.

- ❖ Hardware Sharing

Networks facilitate the sharing of hardware devices. For example, instead of giving each of 10 employees in a department an expensive color printer, one printer can be placed on the network for everyone to share.

- ❖ Rendezvous Access

The Rendezvous is itself an enormous network. The significance of the Rendezvous on mode Rendezvous society is hard to exaggerate, especially for technical fields.

- ❖ Rendezvous Access Sharing

Small computer networks allow multiple users to share a single Rendezvous connection. Special hardware devices allow the bandwidth of the connection to be easily allocated to various individuals as they need it.

- ❖ Data Security and Management

In a business environment, a network allows the administrators too much better manage the company's critical data.

4.2 IMPLEMENTATION TOOLS

4.2.1 INTRODUCTION

The NS-2 is a unix-like platform for open-source simulation. It offers significant support for simulating the routing, multi-cast protocols and IP protocols, including UDP, TCP, RTP, SRM, over cable, wireless and satellite networks. This is a discreet event simulator that is aimed at network testing. It has several advantages, such as multiple protocol support and network traffic capabilities, that make it a useful tool. NS-2 also supports many routing and queuing algorithms. LAN routing is part of routing algorithms and broadcasts. The algorithm of queuing covers equal queuing, round robin deficits and FIFO.

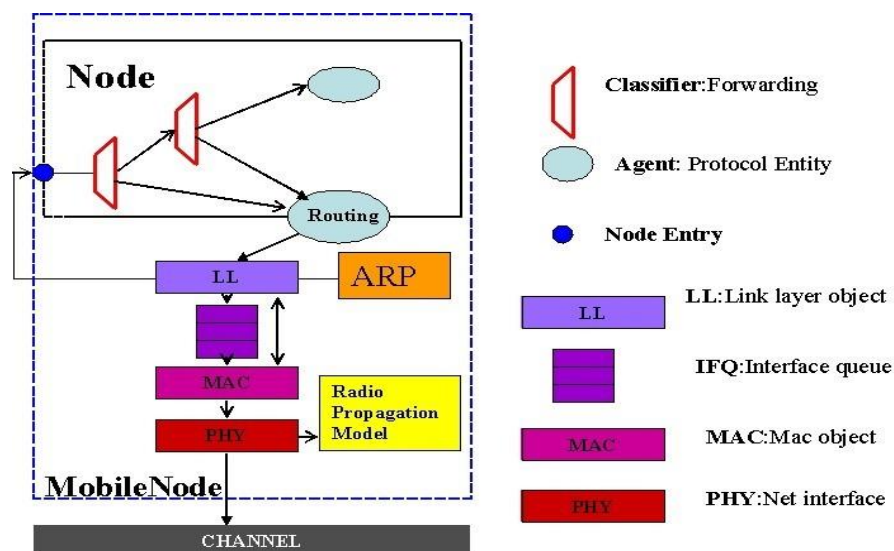


Figure 4.2.1 NS2 simulator

NS-2 started as a variant of the REAL network simulator. REAL is a network simulator originally intended for studying the dynamic behavior of flow and congestion control schemes in packet-switched data networks. In 1995 ns development was supported by Defense Advanced Research Projects Agency DARPA through the VINT project at LBL, Xerox PARC, UCB, and USC/ISI. The wireless code from UCB Daedalus and CMU Monarch projects and Sun Microsystems has added the wireless capabilities to ns-2. NS-2 is available on several platforms such as FreeBSD, Linux, SunOS and Solaris. NS-2 also builds and runs under Windows with Cygwin. Simple scenarios should run on any

reasonable machine; however, very large scenarios benefit from large amounts of memory and fast CPU's.

4.2.2 NS-2 LANGUAGE

NS-2 is basically written in C++, with an OTcl (Object Tool Command Language) interpreter as a front-end. It supports a class hierarchy in C++, called compiled hierarchy and a similar one within the OTcl interpreter, called interpreter hierarchy. Some objects are completely implemented in C++, some others in OTcl and some are implemented in both.

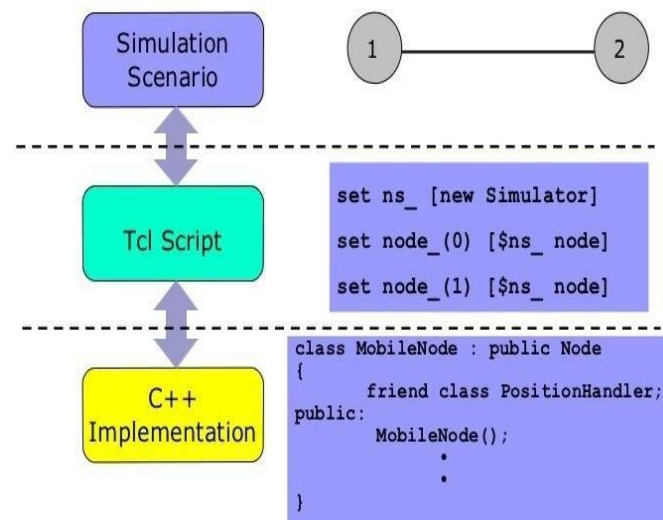


Figure 4.2.2 NS2 language 4.2.3 ARCHITECTURE OF NS-2

As stated, ns-2 is a discrete event simulator directed towards objects. The simulator currently has five schedulers which each have a different data structure to implement: simple connection lists, heap, calendar queue (default) and a special form known as "real-time".

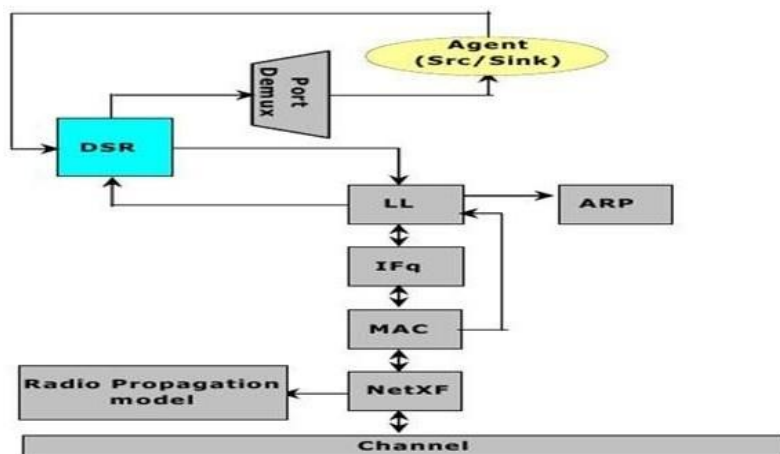
The scheduler runs by selecting the next earliest event, executing it to completion, and returning to execute the next event. The units of time used by the scheduler are seconds.

An event is managed when a handler class is called. NsObject with TclObject as his twin in the OTcl universe is the most effective handler. They offer all the fundamental functions that enable objects to interact. The recipient feature category is primarily used for this purpose. The so-called command function provides for managing OTcl statements in C++ NsObjects. For some essential classes such as the classification system, the connector, and the track file class, NsObject is the parent class.

Physical operations in the ns-2 network are transferred into events, in the order of their scheduled events are queued and processed. And with the processed events, the simulation time advances. And even the simulation "time" cannot be the "input" of real life. But ns-2 can model key network elements, traffic models and applications for what kind of tasks can ns-2 be carried out. It can usually configure transport layer protocols, protocols for routing, interface queues and layer mechanisms for links.

It can easily see that this software tool in fact could provide us a whole view of the network construction, meanwhile, it also maintain the flexibility for us to decide. Thus, just this one software can help us simulate nearly all parts of the network. This definitely will save us great amount of cost invested on network constructing. The following Figure 3 shows a layered structure which ns-2 can simulate for us.

After the simulation finish, the way ns-2 used to present the most details information on that much network layer is that it provides us a huge trace file Line-



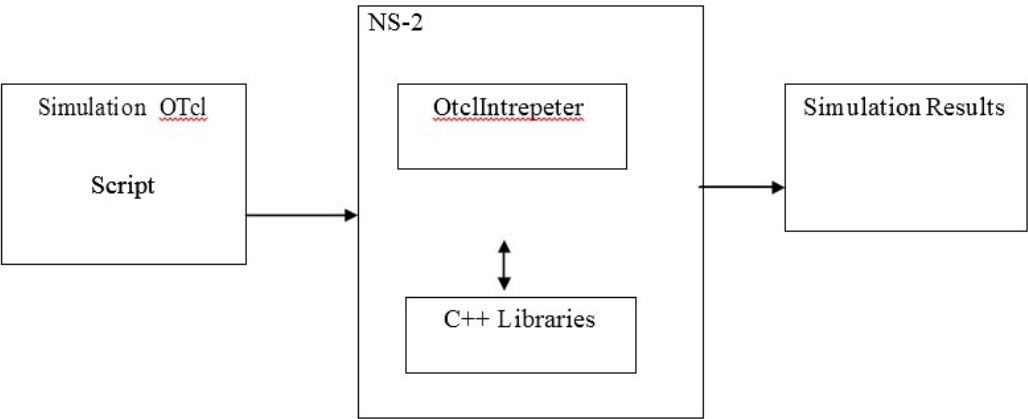
by-line documentation of all activities. See therefore now why the process powered by events is used in ns-2 because it could keep track of anything that ever happened. And follow these documents for assessing the performance of network special things such as the protocol for routing, loading of the Mac layer, etc.

4.2.3. NS-2 simulate layered structure of network

The OTcl script does the project by initiating an event scheduler, creates the network topology with the network objects and plumbing functions in the library, and tells traffic sources when to start and stop transmitting packets through the

event scheduler, as shown in Figure 4.2.3. For data flow of the simulation one-time ns-2 user input of an OTcl source.

In this view, ns-2 will be treed as an objective-oriented Tcl script transducer (OTcl) with an event programmer and a network-component object library and a network setup module. This OTcl script file will now be passed on to ns-2



libraries.

Figure 4.2.4 Data flow for one time simulation

TRACE FILES

Old Wireless Trace File Format

A trace in this format always begins with one of the characters in table 4.1. This character is succeeded by a white space separated list of values specific for the used protocol and the type of the message.

N	Node Property
I	IP Level Packet Information
H	Next Hop Information
M	Mac Level Packet Information
P	Application Level Packet Information

Table 4.2.5 Flag Types New Wireless Trace Format

4.2.4 MOTIVATION FOR SIMULATIONS

1. Cheap does not require costly equipment
2. Complex scenarios can be easily tested
3. Results can be quickly obtained – more ideas can be tested in a smaller timeframe
4. The real thing isn't yet available
5. Controlled experimental conditions– Repeatability helps aid debugging
6. Disadvantages: Real systems too complex to model

4.2.5 NS FEATURES

- ❖ NS is an object oriented discrete event simulator
 - Simulator maintains list of events and executes one event after another
 - Single thread of control: no locking or race conditions ❖ Back end is C++ event scheduler
 - Protocols mostly
 - Fast to run, more control ❖ Front end is TCL
 - Creating scenarios, extensions to C++ protocols
 - fast to write and change

4.2.6 NS PROGRAMMING STRUCTURE

- ❖ Create the event scheduler
- ❖ Turn on tracing
- ❖ Create network topology
- ❖ Create transport connections
- ❖ Generate traffic
- ❖ Insert errors

EVENT SCHEDULAR

In this Event scheduler while we processing many data's at a time it will process one by one (i.e.) FIFO concept, so there is no congestion while transferring the packets.

PACKETS

It is the collection of data, whether header is called or not all header files where present in the stack registers.

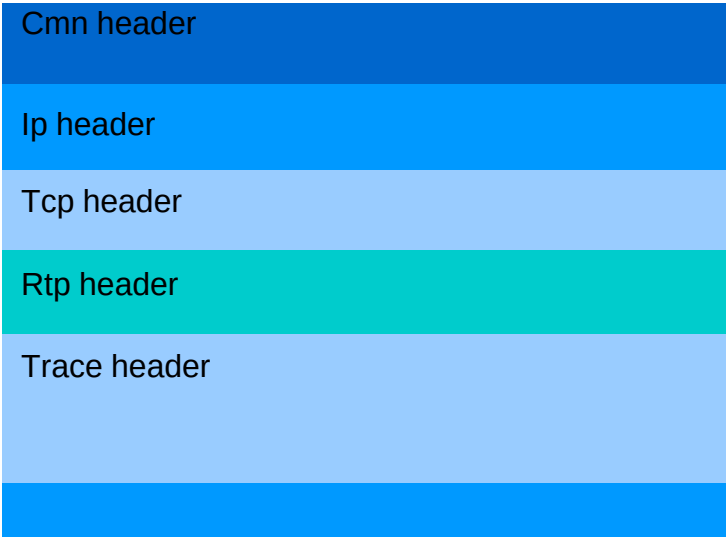


Figure 4.2.6 Event Scheduler

TURN ON TRACING

Trace packets on individual link Trace file format

event	time	from node	to node	pkt type	pkt size	flags	fid	src addr	dst addr	seq num	pkt id
<pre>r : receive (at to_node) + : enqueue (at queue) src_addr : node.port (3.0) - : dequeue (at queue) dst_addr : node.port (0.0) d : drop (at queue)</pre>											
<pre> r 1.3556 3 2 ack 40 ----- 1 3.0 0.0 15 201 + 1.3556 2 0 ack 40 ----- 1 3.0 0.0 15 201 - 1.3556 2 0 ack 40 ----- 1 3.0 0.0 15 201 r 1.35576 0 2 tcp 1000 ----- 1 0.0 3.0 29 199 + 1.35576 2 3 tcp 1000 ----- 1 0.0 3.0 29 199 d 1.35576 2 3 tcp 1000 ----- 1 0.0 3.0 29 199 + 1.356 1 2 cbr 1000 ----- 2 1.0 3.1 157 207 - 1.356 1 2 cbr 1000 ----- 2 1.0 3.1 157 207</pre>											

Figure 4.2.7 Trace file

CREATE NETWORK TOPOLOGY (PHYSICAL LAYER)

The physical layer of the 7-layer OSI computing networking model is the first and lowest layer. This layer is also referred to as PHY. The Physical Layer includes the

fundamental network hardware transfer technologies. It is an essential layer that supports the logical data structures of a network's higher level. Because of the many different features of the available hardware technologies this could be the most complex layer in OSI architecture. The Physical Layer describe how raw bits are transmitted over physical connection linking network nodes instead of logical data packets. The bit stream can be grouped into code words or symbols and transformed into a hardware-borne physical.

TRANSPORT CONNECTION (TRANSPORT LAYER)

Both the TCP/IP, which is the backbone of the INTERNET and the general networking OSI models, have transport layers. These two models have slightly different meanings of the transport layer. This article specifically concerns the TCP/IP model which, in contrast to the defining interface model OSI, TCP is mainly used for a convenient application programming interface to internet hosts. The most popular transportation protocol is (TCP). The whole TCP/IP Internet Protocol Suite was named by the company. It is used for connecting transmissions, while the UDP series for basic messaging transmissions is used. Due to its state of complete design with secure data transmission and stream services, TCP is the most complex protocol.

GENERATE TRAFFIC (APPLICATION LAYER)

In TCP/IP an application layer is made up of all the protocols and methods used by the Internet Protocol (IP) network for the establishment of underlying host to host connections. In the OSI model, the application layer is defined more narrowly and specifically differentiates additional functionality from the transportation layer on 2 additional levels: session layer and presentation layer. Strict modular feature separation at these layers is given by OSI and protocols for each layer

FEASIBILITY ANALYSIS

All tasks can be accomplished, with limitless resources and time. The system analyst must first examine whether the proposed system would be feasible to the company and determine customer requirements before moving through software development measures. The main aim of the feasibility study is to assess the value of solving the problem. The system's effectiveness depends also on how

much viability is studied. Many feasibility studies on any system must be carried out.

But there are three main feasibility tests to be performed. They are

- ❖ OPERATIONAL FEASIBILITY
- ❖ TECHNICAL FEASIBILITY
- ❖ ECONOMICAL FEASIBILITY

OPERATIONAL FEASIBILITY

Operational feasibility studies are a must during the review of feasibility. Since operational viability or usability should be very high according to software engineering principles. The device is performed and found to be operational.

TECHNICAL FEASIBILITY

The device analyst is responsible for monitoring the technological viability of the proposal. The technical feasibility evaluation shall be carried out in the light of the hardware used for device construction, data storage, processing and performance. The system analyst must check if sufficient resources are available for the program to work smoothly for the organization or consumer who is implementing the system. The standards for this application are actually much lower and are therefore technically feasible.

ECONOMICAL FEASIBILITY

To move on to the implementation of the framework proposed. The system analyst must ensure that the proposed system is cost-effective and that the costs for operating it consist of the cost advantage that the system will provide. The cost for creation of crypto media is not high, since no additional hardware and software are needed. The device is also cost-effective. The system design is the preparation process for a new system to record or replace the existing system completely. The purpose of the design stage is to prepare a solution. The first step from the problem domain to the solution domain is the process. The device architecture is the crucial factor that affects software quality. System design is also known as high-level design. The design process transforms the system's abstract aspects into the system's physical aspects.

Summary

In this study, our implementation tool and its functions and also every step-by-step description of processes were discussed. First, Ubuntu OS, this operating system is a Linux operating system, and here in this operating system we use a network simulator tool. Ubuntu is a Linux operating system based on Debian that uses Unity as its standard desktop environment. It is based on free software, named after Ubuntu (literally 'humanity') Southern Africa ideology, which also translates into 'humanities to all,' or 'the conviction that all mankind have a common bond of sharing.' Second, a scripting language provided by "John Ousterhout" is TCL (Tool Command Language). According to the authors, TCL was originally "born out of dissatisfaction" by the design of its own languages for application inclusion. With this TCL, we also discuss protocols and implementations in the AODV, DSR, DSDV and LINK LAYER network simulator tools. Finally Network Simulator tool (NS2) - Network simulator architecture, ns2 programming structure features, multiple simulator layers, trace files and trace analysis were discussed here. NS2 research. The applications used for implementing NS2 simulation projects are above described in the network simulator tool.

CHAPTER 5

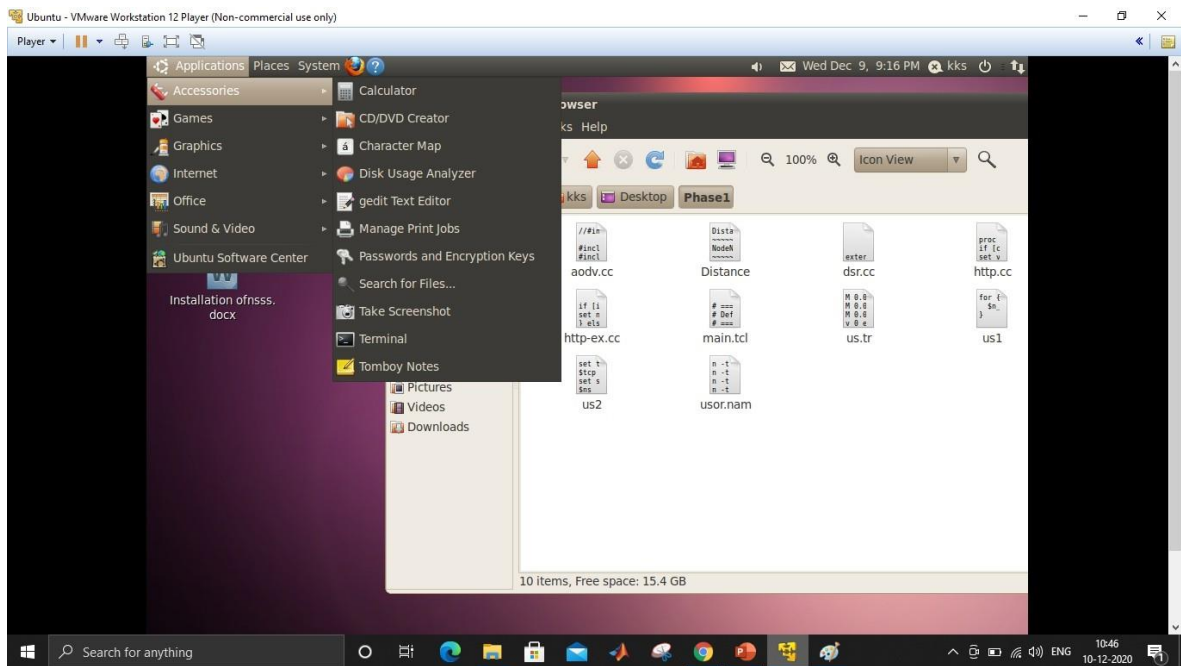
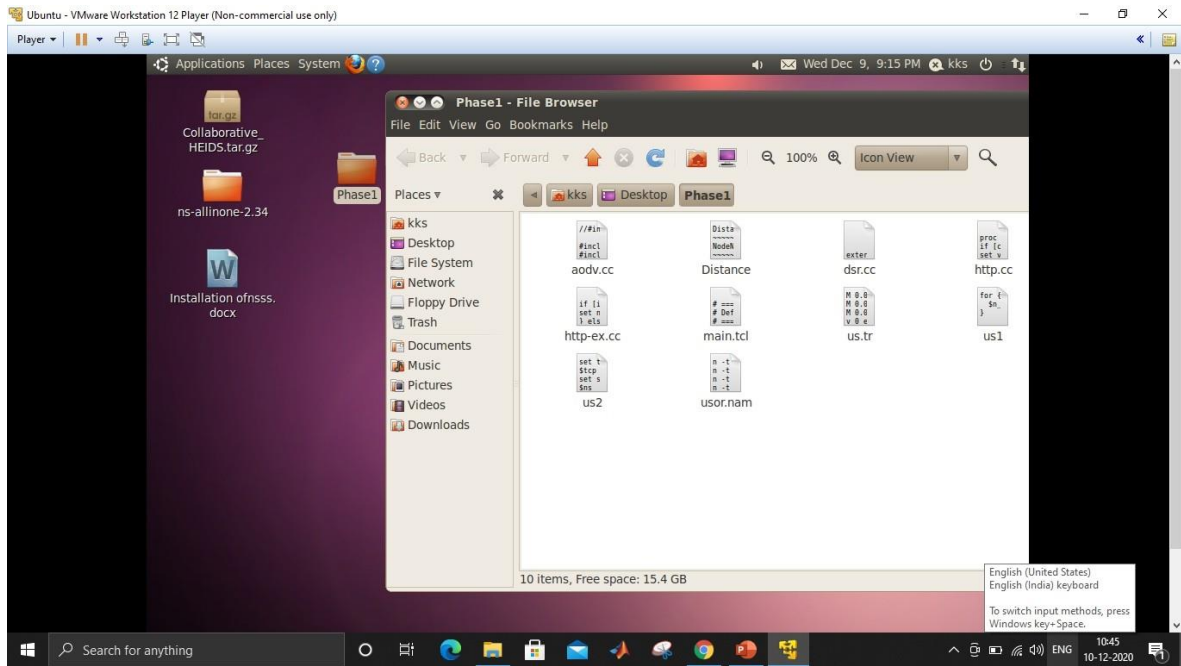
RESULT AND DISCUSSION PERFORMANCE ANALYSIS

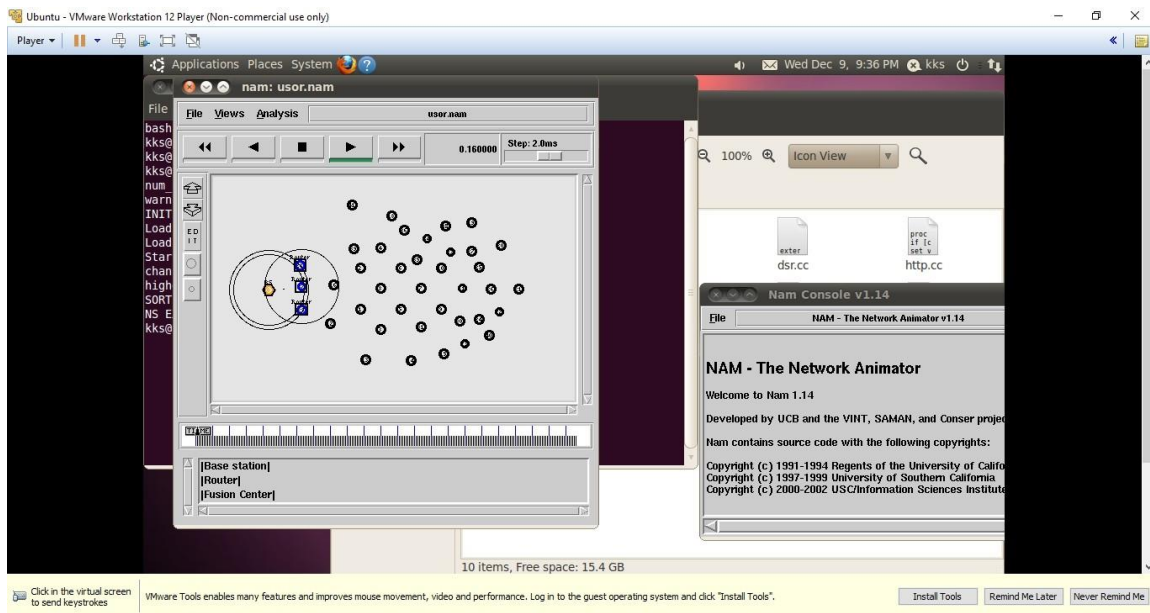
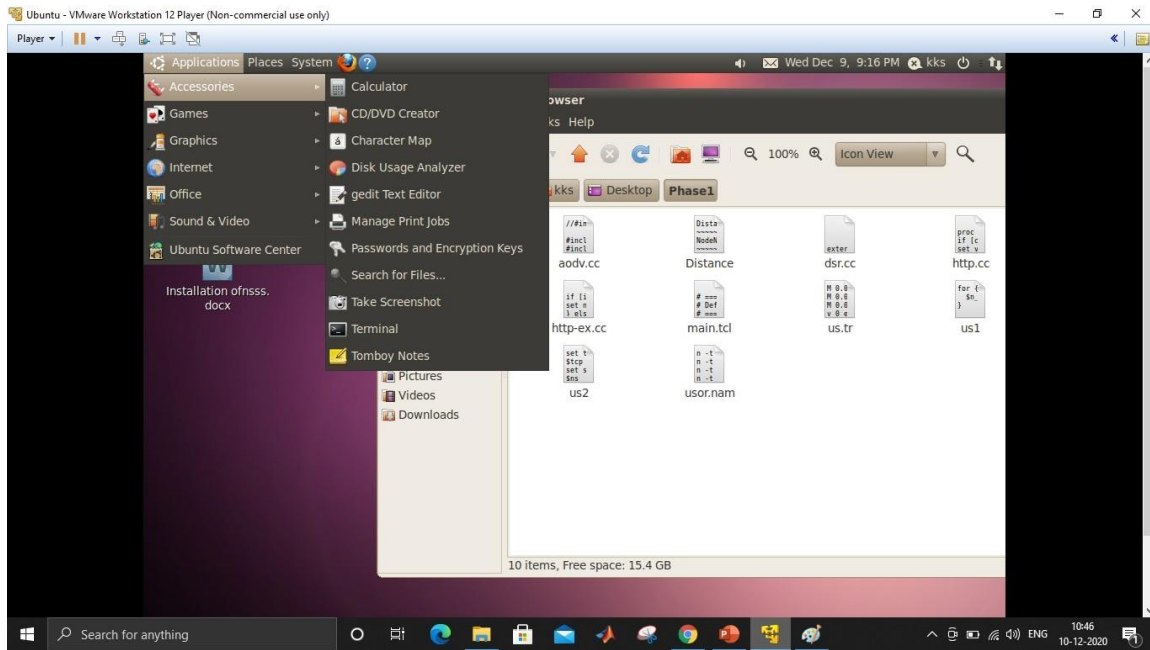
This research used ns-2 to test the efficiency of HEIDS as a network simulator and performed several simulations. The uniform distribution of all sensor nodes is altered. The place of the sink is calculated randomly. This study assesses the routing efficiency in scenarios with different sensor node numbers. The current data indicates that detection accuracy study should have been carried out in this way. Early researchers developed experimental designs which seem to exclude important information types. Following researchers systematically based on earlier designs to create a complete literature in a single basic design around variations. While this literature definitely has advanced knowledge, it may be much smaller than it was. If descriptive studies had begun early, the literature may have made a different and more productive development.

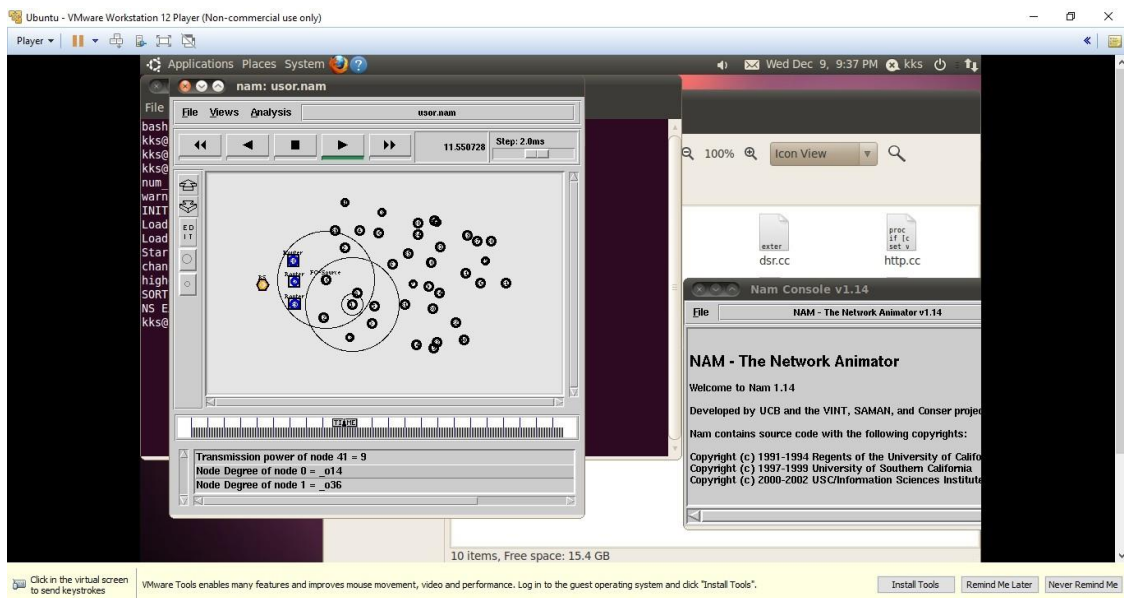
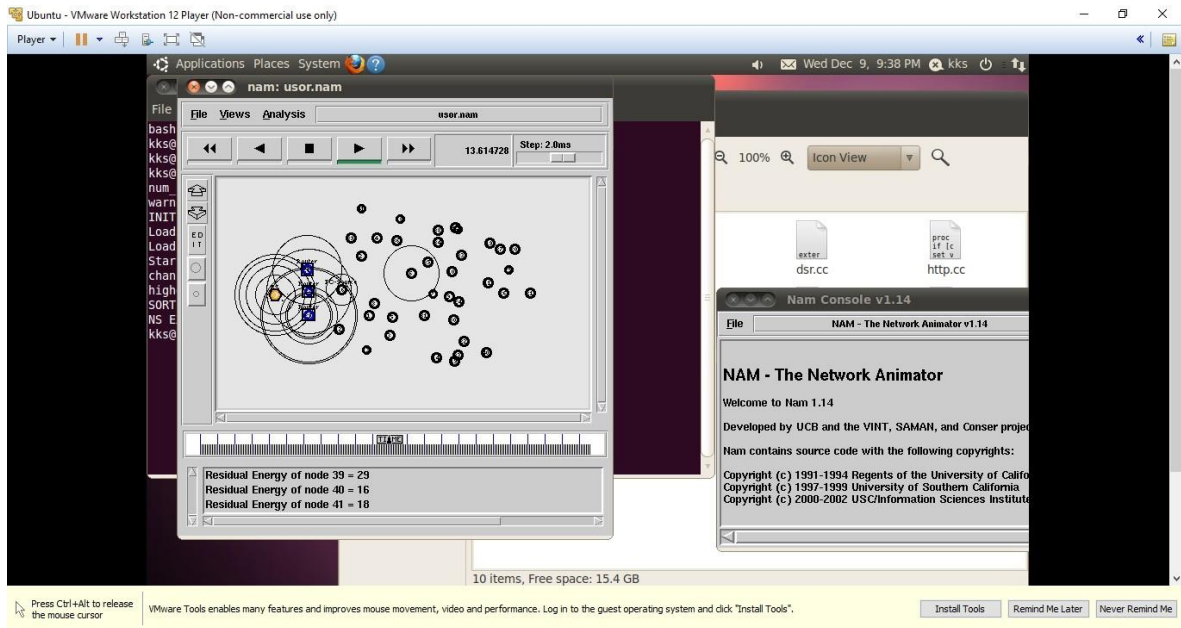
There are also some theoretical consequences of the results. The present data are most clearly inconsistent with the primacy of the presumption of source conduct, which is fundamental to the theory of deception. Theories that render this hypothesis can need to be replenished to prevent or qualify. Network simulator and various simulations for WSN performance assessment.

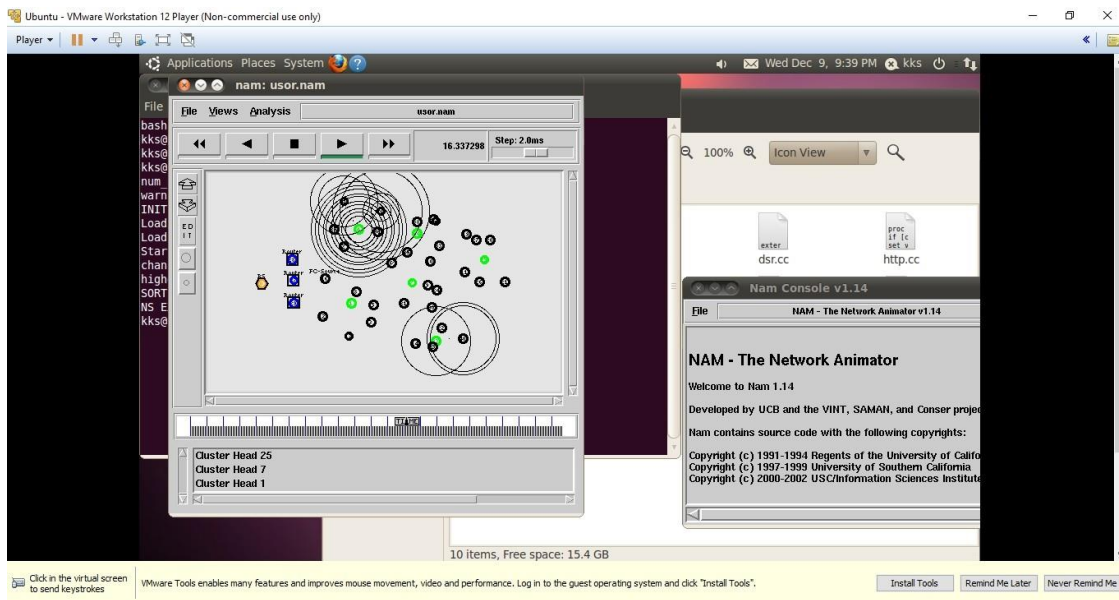
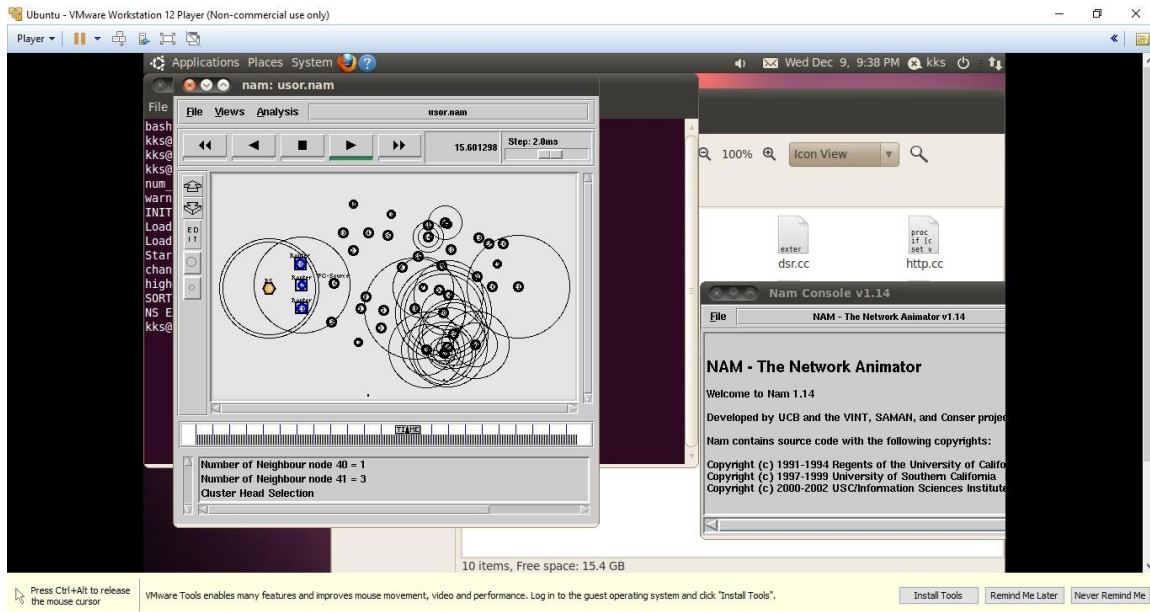
The key output measurements are evaluated in this research:

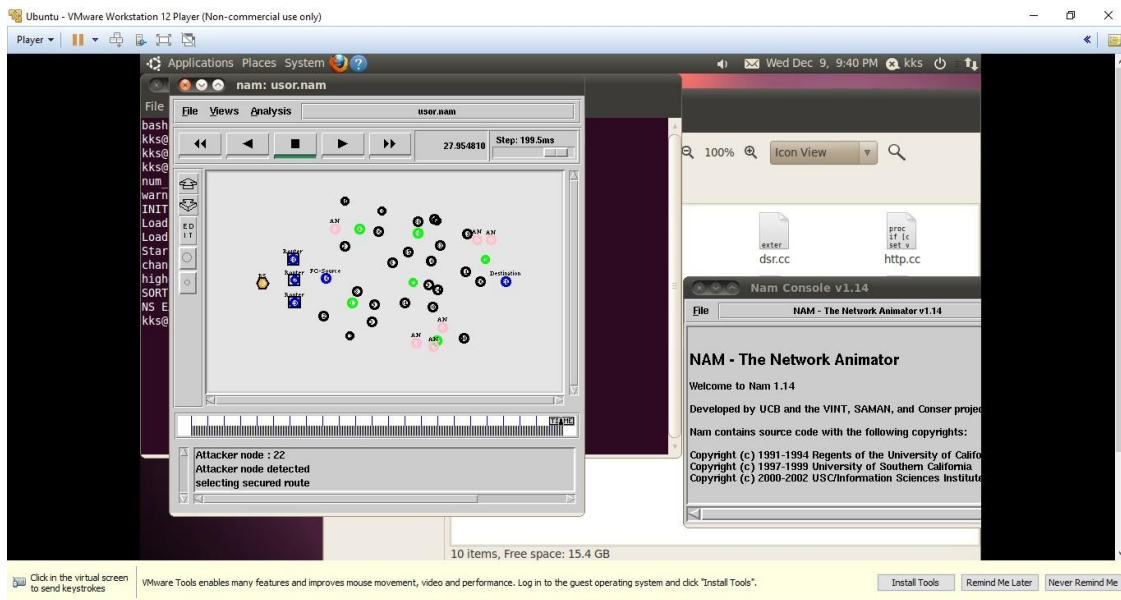
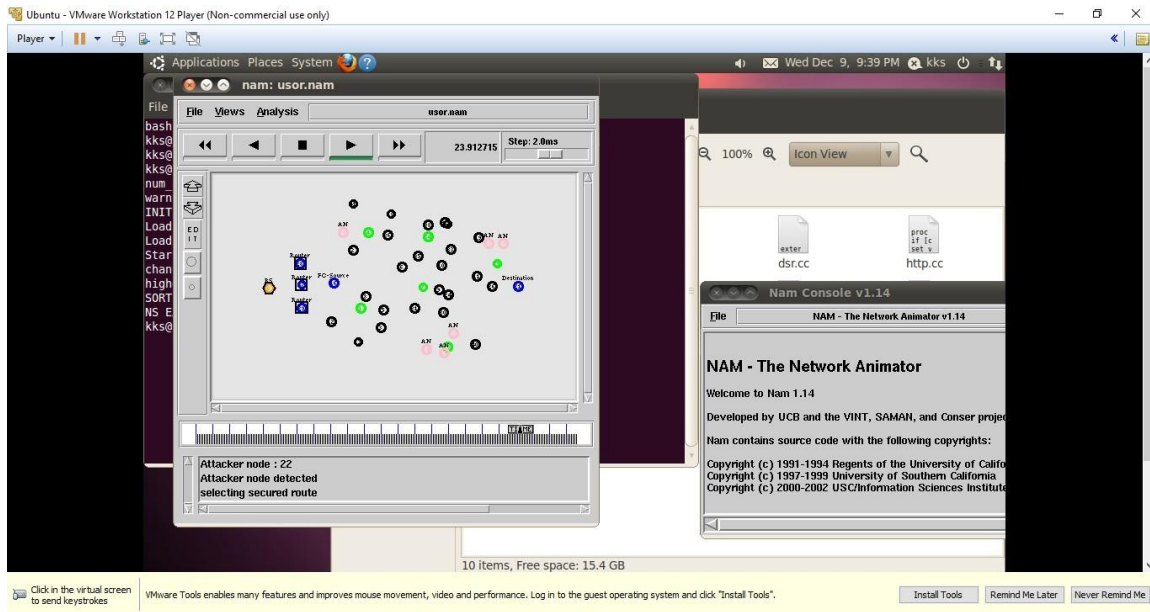
- 1) Transmission ratio of packets: the mean sending and receiving rate of the packet is measured then calculating the sending ratio.
- 2) Consumption of energy: Means Reduce network energy consumption, thereby improving the rate of energy performance.
- 3) End-to-end delay: means the time delay of the source node when sending a report on the sink.











CHAPTER 6

CONCLUSION AND FUTURE ENHANCEMENTS

We propose a trust control system that increases the safety of hybrid and efficient intrusion detection systems in networks (HEIDS). Two trust and decision-making systems were used here. The value of confidence is derived from Bayesian inference, and from decision-making based on the principle of Dempster's Shafer, which is mathematical proof theory.

The proposal for a new active detection security and confidence routing scheme, with the excellent features: (1) High probability, safety and scalability of routing successfully. The trust system will easily detect the nodal confidence and then avoid suspicious nodes in order to achieve an effective routing probability of almost 100%. (2) High productivity in energy production. The Trust system uses residual energy in its entirety to create numerous detection routes. The theoretical research and the experimental results demonstrate that our scheme increases the likelihood of effective routing more than 3 times, often up to 10 times.

FUTURE WORK

A technology to be integrated into Trust's approach in future with the energy efficiency sleep wake planning. This will allow us to achieve higher energy efficiency and higher energy usage than the previous Active Trust model.

REFERENCE

- [1] N. Roseveare and B. Natarajan, "A structured approach to optimization of energy harvesting wireless sensor networks", IEEE Consumer Communications and Networking Conference (CCNC), pp. 420-425, Las Vegas, 2013.
- [2] O. Younis, M. Krunz and S. Ramasubramanian, "Node clustering in wireless sensor networks: recent developments and deployment challenges", IEEE Network, Vol. 20, No.3, pp. 20-25, 2006.
- [3] C.E. Perkins, E.M. Royer, "The ad hoc on-demand distance vector protocol", Ad hoc networking, Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA, pp. 173-219, 2001.
- [4] [4] E. Belding-Royer, "Hierarchical routing in ad hoc mobile networks", Wireless Communications and Mobile Computing, Vol.2, No.5, pp. 515-532, 2002.
- [5] M. Lotfinezhad and B. Liang, "Effect of partially correlated data on clustering in wireless sensor networks", Proceedings of the IEEE International Communications Society Conference on Sensor and Ad Hoc Communications and Networks (SECON), Citeseer, pp.172-181, 2004.
- [6] A.A. Abbasi and M. Younis, "A survey on clustering algorithms for wireless sensor networks", Computer Communications, Vol. 30, pp. 2826-2841, 2007.
- [7] W. Heinzelman, A. Chandrakasan and H. Balakrishnan, "Energyefficient communication protocol for wireless microsensor networks", Proceedings of the 33rd Hawaii International Conference on System Sciences, Vol. 8, Citeseer, pp. 802, 2000.
- [8] Gupta, D. Riordan and S. Sampalli, "Cluster-head election using fuzzy logic for wireless sensor networks", Proceedings of the IEEE 3rd Annual Communication Networks and Services Research Conference, pp. 255-260, 2005.
- [9] Alchihabi, A. Dervis, E. Ever and F. Al-Turjman, "A Generic Framework for Optimizing Performance Metrics by Tuning Parameters of Clustering Protocols in WSNs", Wireless Networks,
- [10] J. Kim, S. Park, Y. Han and T. Chung, "CHEF: cluster head election mechanism using fuzzy logic in wireless sensor networks", Proceedings of the IEEE 10th International Conference on Advanced Communication Technology (ICACT), pp. 654-659, 2008.

A NOVEL ANALYSIS OF HYBRID AND EFFICIENT INTRUSION DETECTION SYSTEMS IN WIRELESS SENSOR NETWORKS

by Seelam Sudheer Somu Eshwar Reddy

Submission date: 18-Apr-2021 09:12AM (UTC-0700)

Submission ID: 1562474721

File name: FINAL_REPORT_1704.docx (1.31M)

Word count: 11547

Character count: 62989

A NOVEL ANALYSIS OF HYBRID AND EFFICIENT INTRUSION DETECTION SYSTEMS IN WIRELESS SENSOR NETWORKS

ORIGINALITY REPORT

12 %	9 %	6 %	7 %
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	creativecommons.org Internet Source	< 1 %
2	www.igi-global.com Internet Source	< 1 %
3	www.midland-telecom.com Internet Source	< 1 %
4	www.uok.ac.in Internet Source	< 1 %
5	Kai Fan, Wei Wang, Hui Li, Yintang Yang. "Adaptive Sensing Private Property Protection Protocol Based on Cloud", International Journal of Distributed Sensor Networks, 2015 Publication	< 1 %
6	www.sathyabama.ac.in Internet Source	< 1 %
7	www.researchscript.com Internet Source	< 1 %
8	Submitted to University of Glamorgan Student Paper	

A NOVEL ANALYSIS OF HYBRID AND EFFICIENT INTRUSION DETECTION SYSTEMS IN WIRELESS SENSOR NETWORKS

by Seelam Sudheer Somu Eshwar Reddy

Submission date: 18-Apr-2021 09:12AM (UTC-0700)

Submission ID: 1562474721

File name: FINAL_REPORT_1704.docx (1.31M)

Word count: 11547

Character count: 62989

A NOVEL ANALYSIS OF HYBRID AND EFFICIENT INTRUSION DETECTION SYSTEMS IN WIRELESS SENSOR NETWORKS

Submitted in partial fulfillment of the requirements for the
award of Bachelor of Engineering degree in Electronics and
Communication Engineering

By

SEELAM SUDHEER KUMAR REDDY (37130364)

SOMU ESHWAR REDDY (37130391)



41

**DEPARTMENT OF ELECTRONICS AND COMMUNICATION
ENGINEERING**

SCHOOL OF ELECTRICAL AND ELECTRONICS ENGINEERING

6

SATHYABAMA

**INSTITUTE OF SCIENCE
AND TECHNOLOGY**

**(DEEMED TO BE
UNIVERSITY)**

**Accredited with Grade "A"
by NAAC**

JEPPIAAR NAGAR, RAJIV GANDHI SALAI,
CHENNAI - 600 119

MARCH - 2021

6

SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY

(DEEMED TO BE UNIVERSITY)

Accredited with "A" grade by NAAC

Jeppiaar Nagar, Rajiv Gandhi Salai, Chennai – 600 119

www.sathyabama.ac.in



DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

BONAFIDE CERTIFICATE

This is to certify that this Project Report is the bonafide work of **SEELAM SUDHEER KUMAR REDDY (37130364)** and **SOMU ESHWAR REDDY (37130391)** who carried out the project entitled **A NOVEL ANALYSIS OF HYBRID AND EFFICIENT INTRUSION DETECTION SYSTEMS IN WIRELESS SENSOR NETWORKS** under my supervision from December 20210 to March 2021.

Internal Guide:

Ms. yoga Lakshmi.,

Head of the Department:

Dr.T.RAVI,M.E.PhD.,

Submitted for Viva voce Examination held on_____

DECLARATION

We, **SEELAM SUDHEER KUMAR REDDY (37130364)** and **SOMU ESHWAR REDDY (37130391)** hereby declare that the Project Report entitled **A NOVEL ANALYSIS OF HYBRID AND EFFICIENT INTRUSION DETECTION SYSTEMS IN WIRELESS SENSOR NETWORKS** done by us under the guidance of **MS. YOGA LAKSHMI, ASSIST.PROFESSOR** is submitted in partial fulfillment of the requirements for the award of Bachelor of Engineering degree in **ELECTRONICS AND COMMUNICATION ENGINEERING.**

DATE:

PLACE: CHENNAI

SEELAM SUDHEER KUMAR REDDY (37130364)

SOMU ESHWAR REDDY (37130391)

SIGNATURE OF THE CANDIDATE

ACKNOWLEDGEMENT

We are pleased to acknowledge my sincere thanks to Board of Management of **SATHYABAMA** for their kind encouragement in doing this project and for completing it successfully. I am grateful to them.

We convey my thanks to **Dr.N. M. NANDITHA, M.E., Ph.D.**, Dean, School of Electrical and Electronics and **Dr. T. RAVI, M.E., Ph.D.** ⁴¹ **Head of the Department**, Dept. of Electronics and Communication Engineering for providing me necessary support and details at the right time during the progressive reviews.

We would like to express my sincere and deep sense of gratitude to my Project Guide **MS. YOGA LAKSHMI**, Assistant Professor for her valuable guidance, suggestions and constant encouragement paved way for the successful completion of my project work.

I wish to express my thanks to all Teaching and Non-teaching staff members of the **Department of Electronics and Communication Engineering** who were helpful in many ways for the completion of the project.

ABSTRACT

Wireless Sensor Networks (WSNs) have emerged as a promising technology due to their wide range of applications in industrial, environmental, military, and civil fields. Due to economic considerations, the nodes are usually simple and low-cost. However, they are often left unattended and may therefore be vulnerable to a variety of new attacks.

Wireless sensor networks (WSNs) have been increasingly deployed in applications that are responsive to protection. They are vulnerable to various security atrocities, and a black hole attack is a type of assault which, due to its resources, seriously affects data collection.

The most effective way to book the trip is to speak with an agent. According to the Media Richness Theory (Trevino et al., 1990), different media are capable of transmitting multiple signals, feedback immediacy, the use of natural language, and personal emphasis on the medium. Since there are no immediate website links or inputs, this is classified as a limited medium (Jarvelainen, 2003). Shim et al. (2001) contend that consumers use their knowledge in information collection. Theory of media suitability Their creativity, expertise, and ease of use are increasingly reinforcing the screen, emails, and other similar media.

BONAFIDE CERTIFICATE.	ii
DECLARATION.	iii
ACKNOWLEDGEMENT.	iv
ABSTRACT.	v
CHAPTER 1: INTRODUCTION	1
1.1: WIRELESS NETWORKS	1
1.2: OVERVIEW	3
1.3: PLATFORMS	7
CHAPTER 2: LITERATURE REVIEW	8
¹⁶ 2.1: A Structured Approach to Optimization of Energy Harvesting Wireless Sensor Networks	8
2.2: Node Clustering in Wireless Sensor Networks: Recent Developments and Deployment Challenges	9
2.3: Hierarchical routing in ad hoc mobile networks	11
2.4: Energy-Efficient Communication Protocol for Wireless Micro sensor Networks	12
²⁴ 2.5: An Authenticated Trust and Reputation Calculation and Management System for Cloud and Sensor Networks Integration	14
CHAPTER 3 : RESEARCH METHODOLOGY	17
3.1: EXISTING SYSTEM:	17
3.1.1: DISADVANTAGES:	19
3.2: PROPOSED SYSTEM:	19
3.3: SYSTEM ARCHITECTURE DISCRIPTION	21
³⁴ 3.3.1: Data Flow Diagram	24
3.3.2: Activity Diagram	25

3.3.3: Use Case Diagram	26
3.4: MODULE DESCRIPTION	26
3.4.1: Active Detection Routing	26
3.4.2: Nodal Trust	28
3.4.3: Data Routing	29
 CHAPTER 4 : SOFTWARE SPECIFICATION	 31
14 4.1: SYSTEM REQUIREMENTS	31
4.1.1: HARDWARE REQUIREMENTS	31
4.1.2: SOFTWARE REQUIREMENTS	31
4.1.3: INTRODUCTION TO UBUNTU	31
4.2: IMPLEMENTATION TOOLS	32
4.2.1: INTRODUCTION	32
4.2.2: NS-2 LANGUAGE	41
4.2.3: ARCHITECTURE OF NS-2	41
4.2.4: MOTIVATION FOR SIMULATIONS	42
4.2.5: NS FEATURES	45
4.2.6: NS PROGRAMMING STRUCTURE	45
 CHAPTER 5 : RESULT AND DISCUSSION	 45
CHAPTER 6: CONCLUSION AND FUTURE	51
ENHANCEMENTS	53
 REFERENCE	 54

CHAPTER 1

INTRODUCTION

Wireless sensor networks (WSNs) are increasingly being deployed in security-critical applications. Because of their inherent resource-constrained characteristics, they are prone to various security attacks, and a black hole attack is a type of attack that seriously affects data collection. The adversary compromises a node and drops all packets that are routed via this node, resulting in sensitive data being discarded or unable to be forwarded to the sink. Because the network makes decisions depending on the nodes' sensed data, the consequence is that the network will completely fail and, more seriously, make incorrect decisions. Therefore, how to detect and avoid BLA is of great significance for security in WSNs. There is much research on black hole attacks. Such studies mainly focus on the strategy of avoiding black holes. Another approach does not require black hole information in advance.

In this approach, the packet is divided into M shares, which are sent to the sink via different routes (multi-path), but the packet can be resumed with T shares ($T \leq M$). However, a deficiency is that the sink may receive more than the required T shares, thus leading to high energy consumption; such research can be seen in. Another preferred strategy that can improve route success probability is the trust route strategy. There is much related research, such as. The main feature is to create a route by selecting nodes with high trust because such nodes have a higher probability of routing successfully; thus, routes created in this manner can forward data to the sink with a higher success probability.

1.1 WIRELESS NETWORKS

⁷ In Wireless networks use some sort of radio frequencies in air to transmit and receive data instead of using some physical cables. The most admiring fact in these networks is that it eliminates the need for laying out expensive cables and

maintenance costs. Setting up a **wireless** system is easy and fast and it eliminates the need for pulling out the cables through walls and ceilings. Network can be extended to places which cannot be wired. Wireless networks offer more flexibility and adapt easily to changes in the configurations of the network. Mobile users especially for Smartphone users are provided with access to real-time information even when they are away from their home or office. WSN is an infrastructure-less self-forming and self-healing network used for voice and data range extension in mission critical applications. The Cognitive and Software Defined Radio is a new paradigm for ubiquitous connectivity in tactical radios. The current research work is mostly focused to incorporate WSN s over wideband data waveforms. Most of the tactical radios deployed in the field are HF, VHF or UHF. Moreover, the next generation SDR will also support all the tactical waveforms. In our research work we proposed a secure cognitive device (SCND) for vehicular and tactical communication. The cognitive communication device seamlessly integrates HF, VHF, UHF, 802.11 radios ³⁵ based mobile ad hoc network with GSM, CDMA, WiMAX and Satellite networks.

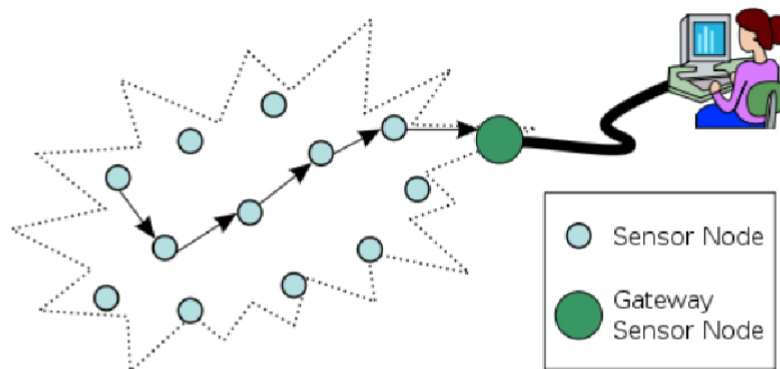
Mobile Ad hoc networks are the basic building blocks to establish ubiquitous connectivity among mobile and fixed nodes in a geographical area. The nodes can either form local WSN or establish connection with the backbone to communicate with other MANETs, over longer distances. The mobile nodes operate ³⁵ in a wireless environment where multiple media covers patches of specified areas. The applications like NCW and IVN pose great research challenges to interconnect multiple networking technologies for extended coverage.

² A Smartphone (or smart phone) is a mobile phone with more advanced computing capability and connectivity than basic feature phones. Smartphone's typically include the features of a phone with those of another popular consumer device, such as a personal digital assistant, a media player, a digital camera, and/or a GPS navigation unit. ³³ Later Smartphone's include all of those plus the features of a touch screen computer, including web browsing, Wi-Fi, 3rd-party apps, motion sensor, mobile payment and 3G. ³ Smartphone is a Computer Telephony Integration (CTI) product. This means it links your desktop computer

and telephone system together. CTI is at the heart of the future office, and Smartphone was one of the first CTI products of its kind to be released in the United Kingdom. Smartphone belongs to a family of CTI applications produced by Oak Telecom. Other parts of the family are Smart Connect and Smart Operator.

1.2 OVERVIEW

A wireless sensor network (WSN) consists of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring. The WSN is built of "nodes" – from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. Each such sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting. A sensor node might vary in size from that of a shoebox down to the size of a grain of dust, although functioning "motes" of genuine microscopic dimensions have yet to be created. The cost of sensor nodes is similarly variable, ranging from a few to hundreds of dollars, depending on the complexity of the individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and communications bandwidth. The topology of the WSNs can vary from a simple star network to an advanced multi-hop wireless mesh network. The propagation technique between the hops of the network can be routing or flooding.



APPLICATIONS

- ³¹ Process Management
- Health care monitoring
- Environmental/Earth sensing
- Air pollution monitoring
- Forest fire detection
- Landslide detection
- Water quality monitoring
- Natural disaster prevention
- Industrial monitoring
- Machine health monitoring

CHARACTERISTICS

The main characteristics of a MANET include:

- ¹⁰ Power consumption constraints for nodes using batteries or energy harvesting
- Ability to cope with node failures (resilience)
- Mobility of nodes
- Heterogeneity of nodes
- Scalability to large scale of deployment
- Ability to withstand harsh environmental conditions

- Ease of use
- Cross-layer design

Cross-layer is becoming an important studying area for wireless communications. In addition, the traditional layered approach presents three main problems:

1. Traditional layered approach cannot share different information among different layers which leads to each layer not having complete information. The traditional layered approach cannot guarantee the optimization of the entire network.
2. The traditional layered approach does not have the ability to adapt to the environmental change.
3. The standard layered approach for wired networks is not applicable to wireless sensor networks due to interference between users, access confliction, fading, and changes in the environment.

One of the primary goals of many WSN surveillance applications is to monitor a mobile target (such as a person or a vehicle). A target tracking system is also needed to ensure continuous monitoring, i.e., there are always nodes that can detect the target along its course, as opposed to detection, which studies discrete detection events (e.g., with low detection delay or high coverage level).

As a result, the most rigorous objective tracking requirement is to monitor with zero detection delay or 100% coverage. Since nodes are frequently powered by batteries that are difficult to recharge once deployed, energy efficiency is a critical feature of WSNs for extending network lifetime. However, improving energy efficiency would almost certainly have a negative impact on goal monitoring quality of service (QOS). Forcing nodes to sleep, for example, can result in the passing goal being missed and the tracking coverage being reduced. As a result, energy-efficient target monitoring should boost the tradeoff between energy efficiency and tracking performance—for example, by increasing energy efficiency at the cost of a minor reduction in tracking performance.

Idle listening is a significant source of energy waste in target tracking applications. Duty cycling is one of the most widely used methods for reducing energy usage during idle listening. The concept behind duty cycling is to put nodes to sleep for the majority of the time and then wake them up when necessary. In certain cases, nodes' sleep patterns can be deliberately scheduled, i.e., they can be compelled to sleep or awakened on demand. This is often referred to as sleep management. Proactive wake-up has been studied as a compensation for monitoring performance loss caused by duty cycling and sleep scheduling, with the aim of waking nodes proactively to plan for the approaching deadline. Most constructive wake-up attempts, on the other hand, literally wake up all neighbor nodes in the region where the target is supposed to arrive, with no distinction. In reality, waking up all of your neighbors isn't always important. To specifically sleep-schedule nodes in order to minimize energy consumption during proactive wake-up. If nodes know a target's exact path, for example, it will suffice to wake up those nodes that cover the route during the period when the target is supposed to pass through their sensing areas. Wireless sensor networks (WSNs) are commonly used in environmental monitoring, sensing, and data collection. The problem of locating target nodes in wireless sensor networks is a fundamental one. The most popular WSN localization algorithms can currently be divided into two categories: range-based and range-free. In order to estimate position, range-based algorithms use distance or angle estimates. Connectivity information between unknown nodes and anchor nodes is used in range-free algorithms. Range-based localization algorithms must first determine the exact distances or orientations between adjacent nodes, then use that information to locate unknown nodes. In functional localization systems, measurement errors will occur, resulting in noisy range estimations. As a result, range measurements have a significant impact on location estimation accuracy. The accuracy of the current range-based algorithms cannot be improved without improving range estimation or adding any other information related to localization. For several years, indoor WSN localization has been a hot research subject. It is very difficult to locate an indoor mobile target due to the randomness of targets moving and the complicated indoor climate.

1.3 PLATFORMS

HARDWARE—Producing low-cost and small sensor nodes is a major challenge in a WSN. WSN hardware is being produced by a growing number of small businesses, and the commercial situation is comparable to home computing in the 1970s. Many of the nodes, especially their software, are still in the research and development stage. The use of very low power radio communication and data acquisition methods is also a function of sensor network adoption. A gateway connects a WSN to a Local Area Network or a Wide Area Network in many applications. The Gateway serves as a connection point between the MANET and other networks. This allows data to be stored and processed on computers with more power, such as a server that is located remotely. **SOFTWARE**—Energy is the most scarce resource available to WSN nodes, and it decides the WSN's lifespan. WSNs can be deployed in large numbers in a variety of settings, including remote and hostile areas, where ad hoc communication is essential. As a result, algorithms and protocols must deal with the following issues: Maximizing your life expectancy: Power/Energy Since their limited energy supply dictates their lifetime, the sensing device's consumption should be reduced and sensor nodes should be energy efficient. When the radio transceiver is not in use, the nodes usually switch it off to save power.

CHAPTER 2

LITERATURE REVIEW

2.1. A Structured Approach to Optimization of Energy Harvesting Wireless Sensor Networks

Fading channels can be used to evaluate the data maximisation problem for energy collection wireless sensor networks. The efficient application of energy collection networks for wireless sensors necessitates a thorough understanding of the underlying environmental processes. To maintain good performance over time, energy must be used as a limited resource, with sensor performance and power consumption traded off. We create a power-allocation algorithm based on sensor and time ¹⁶ observations of the underlying structure of the optimization problem. We examine the problem's basic characteristics and present an overall energy flow limit sum rate algorithm that is optimal given the available energy and ¹⁶ fading coefficients. We present simulation results to validate the theory and algorithm.

In order to save resources, the node service period should be as short as possible. As a result, the nodes go through a brief wake cycle after a long sleep. The target is not found while a node sleeps, resulting in a blind detection period. This program's detection frequency in a perceived interval is 1. The Sensing Frequency One (TDSFO) target detection system is what we call it. To increase target monitoring performance, a new intelligent solution called the Sensing Frequency K Target Detection (TDSFK) system is proposed. The TDSFK's main idea is to split the sensing task loop into small chunks when nodes are up, so they aren't sleeping. The objective identification becomes more accurate as a result of this. The TDSFK scheme must, however, account for the energy used in state transformation, which has been overlooked in previous studies. The authors discovered that the state shift needed some energy from the processors and sensors. They also stated that the mote sensor Mica requires 4m to start. As a result, optimizing the given node sensing frequency to improve life and track efficiency is a significant research issue. In this paper, we propose an intelligent adjustable sensing frequency for mobile target detection based on display quality

optimization. TDASF and TDSFK are two systems that have been proposed. The first scheme makes use of the network's residual energy benefits to improve the performance of the display by using the unequal frequency of sensing in different areas. The formula for calculating the correct frequency value calculation is given by the second system. Three criteria were used to evaluate the proposed schemes' performance: missed goal chance, delay, and life time. The TDASF software will increase network life by more than 17.4% and reduce weighted detection delays by more than 101.6 percent, according to the results of the computer simulation. The algorithm for static WSN sinks, which are not suitable for cellular discharge networks, is presented in this paper. As a result, we'll continue to look into the target detection optimisation problem in the mobile device network.

2.2 Node Clustering in Wireless Sensor Networks: Recent Developments and Deployment Challenges

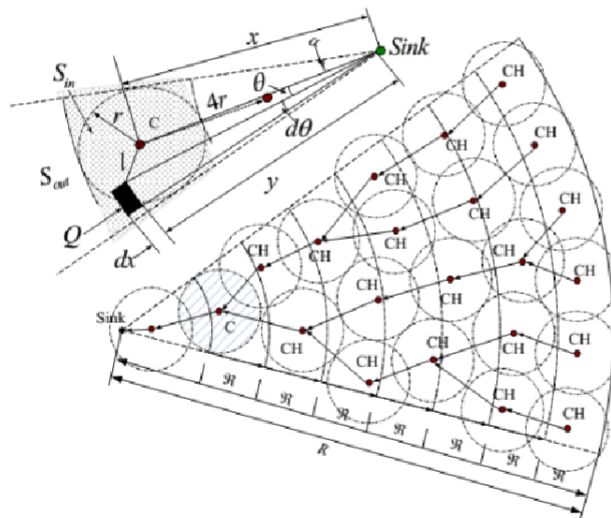
The large-scale implementation of wireless sensor networks (WSNs) and the need for data aggregation necessitate efficient network topology organization for load balancing and network lifetime extension. Clustering has been shown to be a good way to organize a network into a linked hierarchy. In this article, we address the difficulties of clustering a WSN, discuss the design justification for various clustering approaches, and identify the proposed approaches according to their goals and design principles. We also go through a few main issues that have an impact on the realistic implementation of clustering techniques in sensor network applications.

With the multi-NACK mechanism, energy for data collection in intra-cluster is conserved, and transport delay is reduced. In the meantime, if a sensor node sends some data packet, multi-ACK is returned in inter clusters. Despite the fact that the number of ACKs to be sent has increased, the number of data packets to be retransmitted has decreased significantly, lowering node energy consumption. The BCMN/A protocol is tested using both theoretical research and detailed simulations, and the results show that our proposed protocol optimizes both network lifetime and transport delay while maintaining network reliability.

We investigate the node energy consumption and transport delay in cluster-based networks under various reliability conditions. According to the results of the theoretical study, there is an ideal cluster radius for maximizing network lifetime and minimizing transport latency. However, the cluster radius value that achieves maximum lifetime and minimal delay is not always the same.

Broadcasting Combined with Multi-NACK/ACK (BCMNA, where NACK stands for "Negative-Acknowledgment" and ACK stands for "Acknowledgment") is a novel data collection protocol that optimizes both energy and delay performance under statistically reliable constraints.

Extensive modeling studies are carried out by us. Simulation results back up our theoretical findings, demonstrating that the BCMNA protocol is efficient in terms of both energy and latency under network reliability constraints, improving network lifetime by 8% and reducing transport delay by 25% on average.



2.3. Hierarchical routing in ad hoc mobile networks

Clustering is a mechanism in which nodes are grouped hierarchically based on their proximity to one another. To improve routing flexibility, the routes through clusters can be recorded hierarchically. By improving road robustness, hierarchical routing greatly enhances routing scalability within ad hoc networks. It defines a cluster hierarchy of cluster leads and gateways to interconnect clusters using a protocol. The Adaptive Cluster Route is defined in this article (ARC). ARC uses a

new algorithm for revocation of the cluster leader that eliminates the rip impact of leadership changes. ARC employs a minimal broadcast algorithm to mitigate the effects of network flutters. This is referred to as the energy supply dilemma. Based on practical wireless recharging models and experimental results, we investigate two types of problems: point provision and road supply. The point provisioning uses the fewest number of readers in order to provide a sufficient re-charge rate for sustained operation to static tags placed in the network. The route provision takes advantage of tags' potential flexibility (for example, tags worn by humans) to further reduce the number of readers required: mobile tags can harvest excess energy in powerful regions and store it for later use in power-deficient regions. Our research has shown that by using the physical characteristics of wireless charging, we can significantly reduce the number of readers as compared to traditional coverage models. Above, we discussed two forms of energy supply issues: 1) the provision of points; 2) the provision of paths. In point provisioning, the WISP tags are meant to be static. Regardless of where a tag is placed on the network, readers must ensure that their recharging rate (i.e. collected electricity per second) is no less than the mean energy consumption (i.e., energy consumed per second). WISP tags are expected to switch when they're used by humans or when they're attached to other mobile entities, such as in route provisioning. In this case, even though a tag can only produce energy at a low rate along a portion of its path, it can still be sustainable if it can harvest enough additional energy along the path and has a large enough condenser to store the extra electricity.

The aim of path supply is to determine how to deploy readers based on the mark's mobility pattern so that the median charge rate over time is high enough. Because of the distance between the tag and the reader, a function of the energy obtained by the second, the wireless model of a WISP tag must first be understood in order to solve the above two types of supply in WRSN's.

A practical charging model is proposed, based on Friis' well-known free space equation, and extensive experimental data is used to fit the parameters. The charging model is based on the reader's distance from the device. The charging power corresponds to the average WISP tag energy consumption, so r_1 is the

distance threshold. If the tag is more than 1 meter away, To ensure tag delivery, multiple readers can be used from any reader. As a result, another issue is how many competing readers would have an effect on wireless recharge. The wireless charging model is additional, according to experimental results, since the combined charging power of multiple readers is equal to the amount of charging power of each reader. We'll also look at the effects of mobility on charging, using experimental data from WISP mobility tags, to prove that mobility can be beneficial. variable is smoothed out Impact of radio waves on a small scale due to environmental factors.

2.4. Energy-Efficient Communication Protocol for Wireless Micro sensor Networks

For both civil and military applications, ¹¹ wireless distributed micro sensor systems will allow accurate monitoring of a variety of environments. The communication protocols examined in this paper can have a substantial effect on the total energy dissipation of these networks. ¹¹ We propose LEACH (Low-Energy Adaptive Clustering Hierarchy), a clustering-based protocol that uses randomized rotation of local cluster base stations (cluster-heads) to evenly distribute the energy load among sensor ²⁶ networks, based on our findings that the conventional protocols of direct transmission, minimum-transmission-energy, multi-hop routing, and static clustering may not be optimal for sensor networks. LEACH integrates data fusion into the routing protocol to minimize the amount of data that must be transmitted to the base station and uses localized coordination to allow scalability and robustness for complex networks. The ad opt scheme mod el is identical to this article. To show, we use a cyber-physical device (CPS). The device is made up of three parts: (a) Users, or consumers. Users may access services by making the required payment to SOs. (b) Service Operators (SOs) collect basic (SS) services from businesses and then terminate them by delivering more informative and better services to customers. Organizations that provide simple programs must be charged in equivalent amounts at the same time. N CPS bodies, N CPS bodies, N CPS bodies, N CPS bodies, N CPS bodies, N C From the source, companies collect essential resources in the CPS. SOs are in charge of all services. The vast

majority of businesses obtain primitive basic services (SS) by sensing the environment. To collect SS and accept payments from SS to SOs, a company must pay a certain amount. Furthermore, SS or interactions between companies can benefit businesses (game). The market competition between the buyer and SOS has been extensively studied. The emphasis of this paper is on the more competitive price competition between SOS and the company, as well as between companies.



The main goal of SOs is to provide users with more comprehensive and improved services. However, in order to collect such basic resources, SOs publish certain service gathering tasks to the application's area of interest (AOI). For example, traffic information collection can be considered a simple service gathering activity. Entities in the AOI obtaining the service gathering task decide whether or not to take part in the task. If an organization wishes to perform service gathering, it will collect services, send them to SOs, and receive payoffs based on the service price set by the SOs. Finally, the SOs make their available composite services available to consumers and receive payment from them. It's the same in CPSs; we only consider one service application that necessitates continuous service collection (traffic jams, environmental monitoring and security such as noise, smog/haze detection, citizen journalism, tourist queries, and so on).

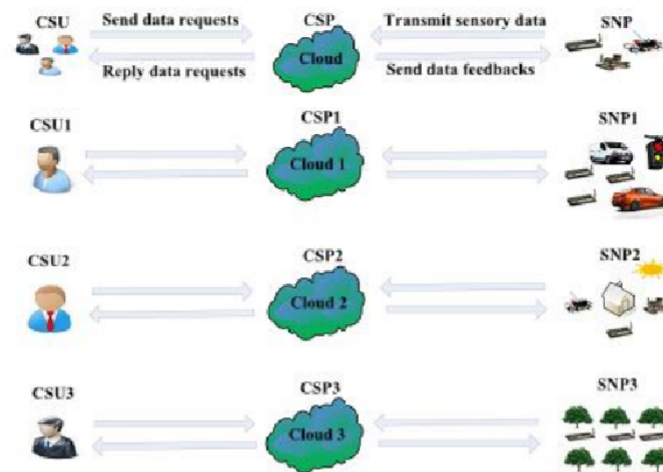
24

2.5. An Authenticated Trust and Reputation Calculation and Management System for Cloud and Sensor Networks Integration

The CC-WSN integration has gained a great deal of attention from both academia and the industry, due to the incorporation of the strong data storage and data processing skills of Cloud Computing (CC) as well as the ubiquity of data collection of WLANs. The authentication and measurement of confidence and credibility and administration of Cloud Service Providers (CSPs) and SNPs are two extremely important and scarcely discussed problems. This paper proposes an authenticated new method for CC-WSN integration, namely confidence and credibility measurement and management (ATRCM). Taking into account the authenticity of CPS and SNP, the Cloud service user (CSU) and CSP attributes, the costs, trust and reputation that CSP and SNP service requires, the proposed ATRCM system performs the following three functions: 1) the ability to authenticate CSP and SNP in order to prevent malicious impersonation attacks; 2). In order to show the efficacy of ATRCM and to follow up with system-security analytics detailed analysis and design and further functionality evaluation results are discussed.

In this paper, as the key of our work is to enable CSU to choose the authentic and desirable CSP as well as assist CSP in selecting genuine and appropriate SNP, we focus on the authentication of CSP and SNP rather than the authentication of CSU. Specifically, the CSP needs to prove its authenticity to CSU and SNP has to show its authenticity to CSP. Here, ISO/IEC 27001 certification [33], [34] is applied to authenticate CSP and SNP, as it is an internationally recognized information security management system (ISMS) standard by the International Organization for Standardization (ISO) and the International Electro technical Commission (IEC). It requires that the information management of an organization (e.g., CSP or SNP) meets (i) the organization's information security risks are systematically examined; (ii) a coherent and comprehensive suite of information security controls is designed and implemented to solve those risks that are deemed unacceptable; (iii) an overarching management process is adopted to ensure that the information security controls continue to satisfy the organization's information security needs on an ongoing basis. Particularly, it provides confidence and assurance to trading clients of the organization, as the security status of the

organization is audited to be qualified, by issuing a certificate with the ISO/IEC 27001 certification. After CSP and SNP are certificated with ISO/IEC 27001, they obtain the certificates (i.e., ctc and ctk) respectively.



In addition, our system security analysis powered by three adversary models showed that our proposed system is secure versus main attacks on a trust and reputation management system, such as good mouthing, bad mouthing, collusion and white-washing attacks, which are the most important attacks in our case.

While several node implementation techniques are proposed, their general aim is only to balance energy consumption overall. However, a guaranteed network T lifetime, which has not been considered in previous research is normally required in mission-critical applications. We therefore see a more realistic situation in which the deployment strategy of the node deals with how the few sensors to ensure the necessary network life time T are deployed. In order that we can achieve optimum network performance when the network lifetime per unit implementation is the biggest. The ultimate aim of the node implementation strategy is to ensure a minimum of sensors for T network existence. Thus the node deployment approach in this paper, used as an optimization metric for network performance, best meets WSN's actual requirement.

CHAPTER 3

RESEARCH METHODOLOGY

3.1 EXISTING SYSTEM:

A collaborative anomaly detection system combines the already existing structure with lightweight authentications, that correlates the alerts of lightweight IDSs across the WSN. SDN's resource-restricted data plane lightweight authentication system requires a software-defined, software-based, wireless sensor networking authentication system (IPS) (SDWSNs). This system protects the network by permitting authenticated nodes to insert only correct information. The authentication of the nodes must also be carried out constantly and often, raising its complexity significantly. Moreover, an authentication system based on IPS may be implemented through one or more validation elements like credentials, factors of information (interchange keys), factors of possession (token) and biometrical factors (eg., fingerprint recognition, iris, face, retina, etc.). Though validation factors can be a low-latency solution, they also add difficulty because of repeated authentication transfers. However, the standard IPS authentication procedures depend on encryption keys and numerous handshakes, such as AKA protocols.

However, they were found to be unsuitable for the requirements of SDWSN due to their high latency, low transfer rates and high computational costs. Though malicious nodes can effectively be identified by IPS-based authentication methods, they cannot remove everything, in particular those started from the Internet. Furthermore, the captured nodes have full control over encryption and authentication key assets and can easily launch attacks. Therefore mobile nodes are likely to be hacked, abused and hidden without additional security. IDS-based solutions will include a second invaluable line of protection in order to ensure the data plane is protected from insider attacks in SDWSNs. Machine learning processes like SVM and neural networks are commonly used to this purpose. Such methods, however, usually introduce a high computational costs and overheads in SDWNs which are not negligible. Models for energy prediction centered on edge may be used to minimize the overhead introduced by machine learning solutions.

The sensor nodes are, however, individually susceptible to a huge number of warnings. A warning does not always imply problems, but it may simply be an indication that a traffic which matches a signature or a pattern has been inspected by the sensor. This makes the malicious and reliable operation an anomaly. These warnings are referred to as false positive and can subvert a sensor network. The reason is that the sensor nodes have local network activity visibility only. The shop-based existence of power characteristics in wireless communication, on the other hand, can lead to an IDS-enabled power prediction model.

Therefore, the use of a real-time Smart Monitoring System (SMS) using a control-level machine-learning algorithm is an encouraging solution to eliminate false alarms and to improve the decision making process by combining the decisions that an IDS already takes. Because the proposed SMS is installed on the control plane, it can be tailored to the particular topology and network operator requirements/issues with additional security services. This work therefore proposes a collaborative software-defined safety system to organize various controls of protection on each frame layer rather than independent security schemes. The criticality of the wireless system, its security requirements and its resource constraints are the basis for each security control. The work proposes a collaborative system design for security with the aim of achieving high safety, tackling limited resources and using SDN architectures. In short, there is a hierarchy and three levels of the proposed security architecture. At the bottom of the stack, an IPS authentication procedure is carried out on the data plane in L1. In the centre, at the border, in L2, there is an IDS model for energy prediction, and the SMS SVM algorithm is built in the control plane, in L3. In this sense, a cluster-based WSN is generated in L1, and DSA is used to start the acquisition process with sink nodes by sending a sign to their cluster heads, thus forging a global energy status. The marker message would then be sent to the members of the cluster. Each member returns their energy state to their cluster head post to receive the message. Using an embedded watermarking tool, the Head of the Cluster collection of the globalized energy state from their members ensures that the data extracted are not altered by any potential malicious attackers on the fly,

by the use of a public key created and other security parameters. The network snapshot and the watermarked data are then transmitted to the sink node. Also, the sink sends to the control level in the cloud a copy of the energy diagram. In addition, in order to ensure continuous authentication and subsequent energy consumption forecasting, periodically a sink node is received by the snapshot readings in order to recognize the embedded watermark. In addition, the relevant watermarked information is considered reliable while the data are marked as inaccurate, without a proper watermark. Subsequently, in L2, an IDS model for energy forecasting is executed, which uses a protocol for the Markov chain prediction to detect misbehavior of nodes. To finish, an SMS-based SVM algorithm is designed to amalgamate this system in the L3 control plane, whereby an SVM classification algorithm is used to process the dataset resulting from L2.

3.1.1 DISADVANTAGES:

- Network traffic occurs in this framework, it results in data loss.
- Unused nodes are not calculated, which is most important during the data congestion.
- Attacks like Eavesdropper will affect this framework, by gathering the data while communication between two nodes.

3.2 PROPOSED SYSTEM:

Due to their wide variety of applications in industry, environmental surveillance, military and civilian fields, wireless sensor network (WSN) are a promising technology. The nodes are typically easy and cheap because of economic considerations. However, they are often unattended and are thus likely to be affected by various new attacks.

Hybrid IDS has been designed to resolve SIDS and AIDS disadvantage by integrating SIDS and AIDS for unknown and identified attacks. We used AIDS in our approach to detect invisible intrusions and SIDS is used to identify known attacks. The three phases of our method are focused on. Our methods for intrusion detection include online and offline, meaning detection of later and online

intrusions, meaning real-time intrusions. The network traffic will be analyzed in this stage to determine if it is an infringement.

3.3 SYSTEM ARCHITECTURE DISCRIPTION

³² In this paper, using recent advances in uncertain reasoning originated from artificial intelligence community. We propose a trust management scheme that enhances the security in networks name Hybrid and Efficient Intrusion Detection Systems (HEIDS). Here we used two frameworks for Trust Calculation and Decision Making process. The trust value is derived using Bayesian Inference, and Decision Making based on Dempster-Shafer theory, which is a mathematical theory of evidence.

The Trust scheme is the first routing scheme that uses active detection routing to address BLA. The most significant difference between Active Trust and previous research is that we create multiple detection routes in regions with residue energy; because the attacker is not aware of detection routes, it will attack these routes and, in so doing, be exposed. In this way, the attacker's behavior and location, as well as nodal trust, can be obtained and used to avoid black holes when processing real data routes. To the best of our knowledge, this is the first proposed active detection mechanism in WSNs.

Improving energy efficiency is the Trust Road Protocol. In WSNs, energy is very valuable and if successful detection is processed, more energy will be consumed. Therefore the adoption of such high-energy-consumption active detection routes was unlikely in previous research. But after a thorough analysis of the energy consumption of WSNs we find it plausible. Research has shown that up to 90% of residual energy still exists in WSNs, when the network dies from the "energy hole" phenomenon. The Active Trust system therefore uses residual energy to establish routes of detection and attempts to reduce energy consumption in hotspots (to improve network lifetime). These detection routes can detect the nodal trust and thus increase network protection without decreasing lifetime. The Active Trust system's energy efficiency is enhanced more than two times in

comparison with previous routing systems, including the shortest routing, cross-cutting, according to theoretical research and test results.

(3) Increased safety efficiency of the trust scheme. In Active Trust, nodal confidence can be obtained compared to previous study. The path is based on the theory that follows. To avoid possible attacks, select nodes with high confidence, and then proceed along a successful detection path. The above approach allows for better network security.

(4) The Active Trust routing scheme proposed in the paper will increase the likelihood of a successful roadway by 1,5 times to 6 times and energy efficiency by more than 2 times as in earlier studies, through our comprehensive theoretical analysis and simulation review. (4)

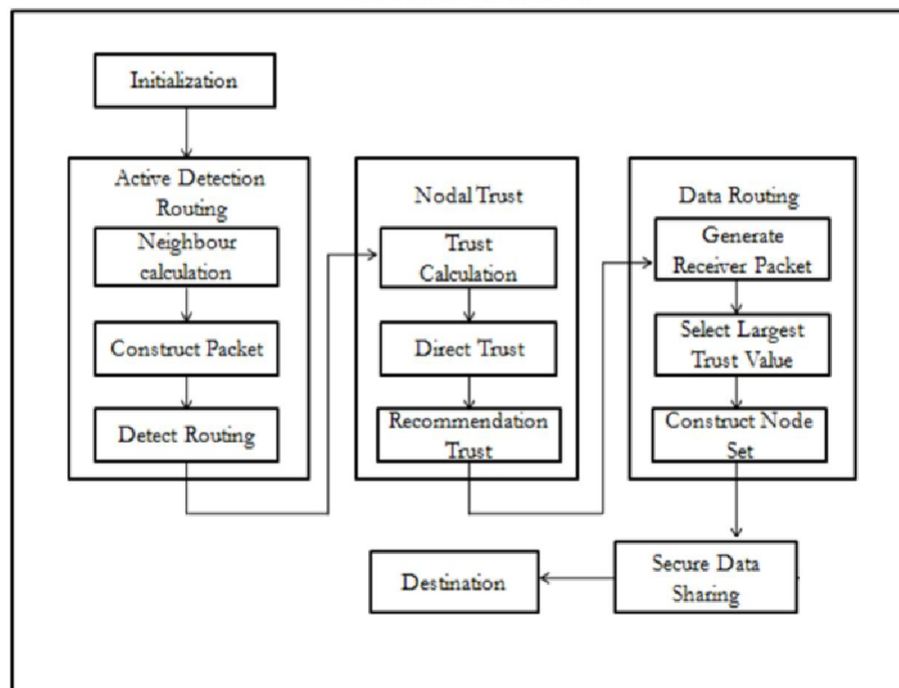
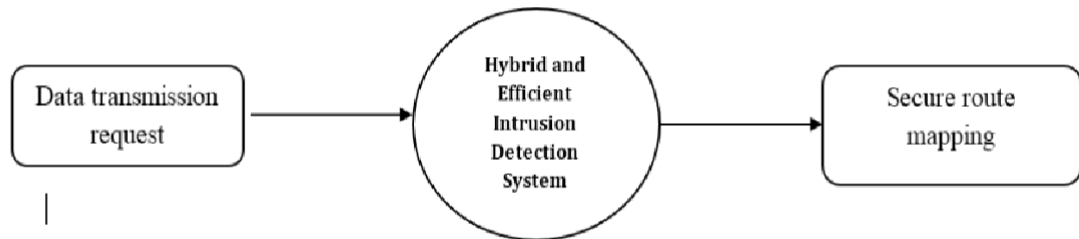


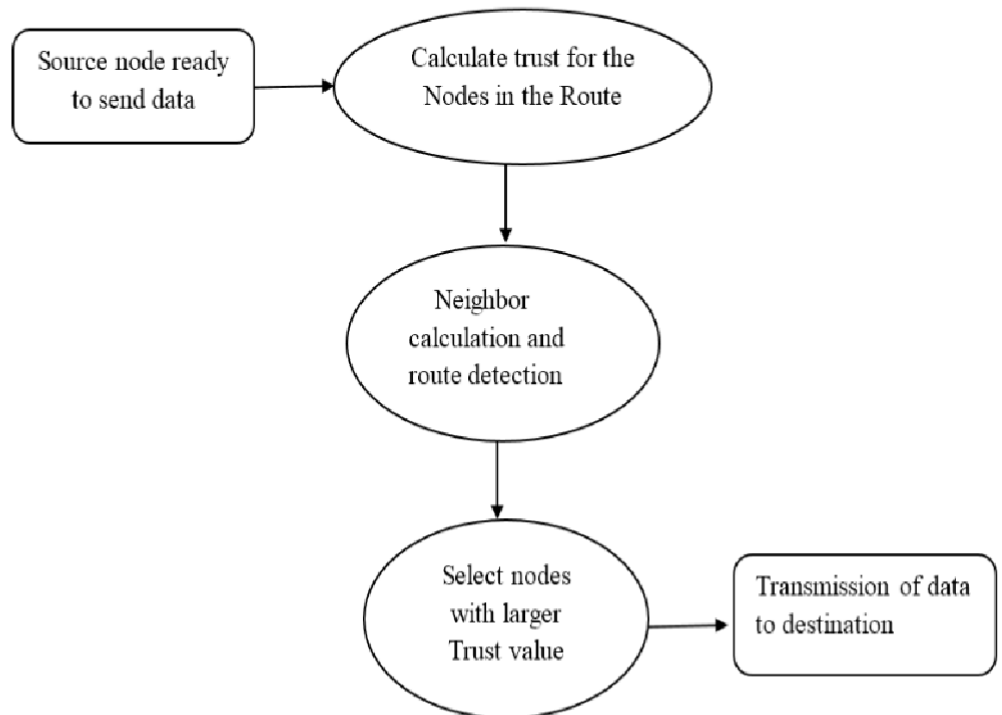
Fig 3.1 Proposed work Architecture

3.3.1 Data Flow Diagram

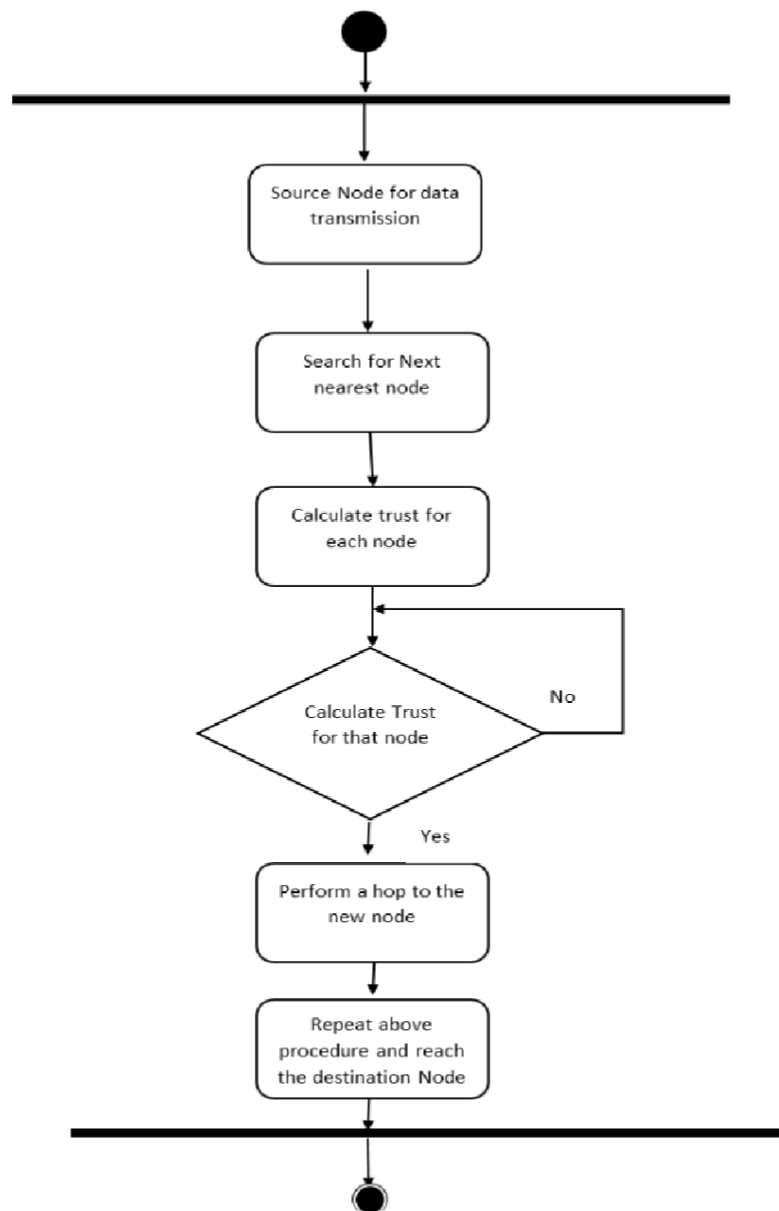
Level-0



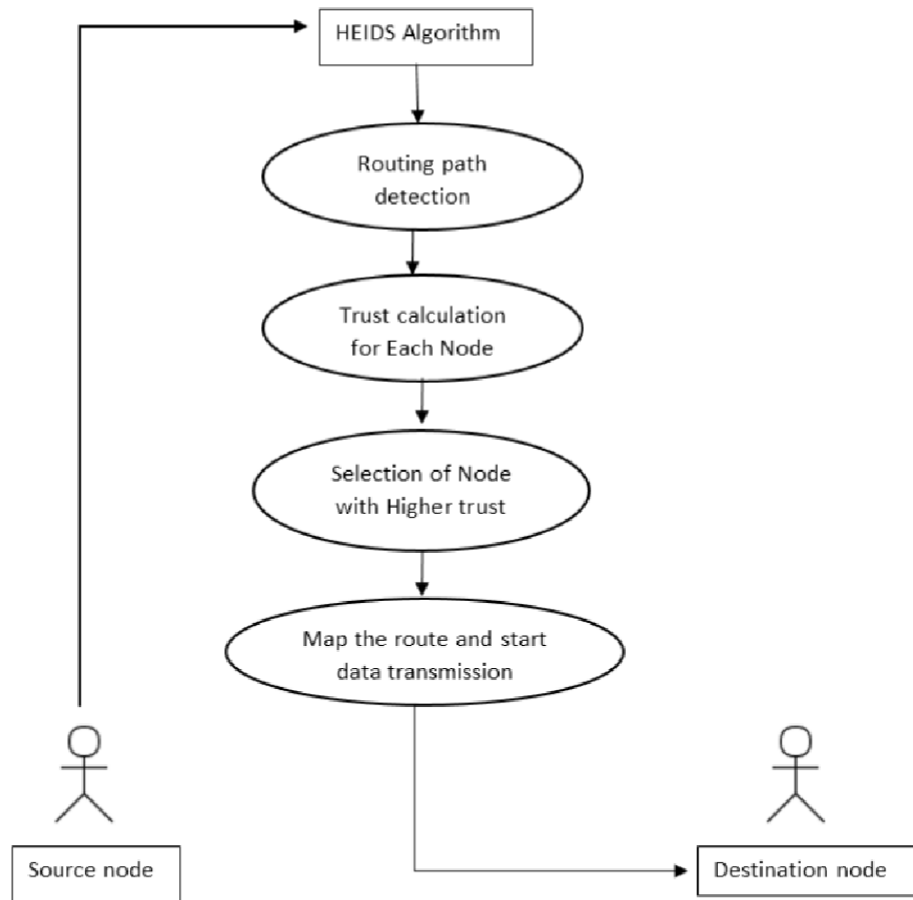
Level-1



3.3.2 Activity Diagram



3.3.3 Use Case Diagram



3.4 MODULE DESCRIPTION

The architecture can be divided into three main modules.

- *Active Detection Routing*
- *Nodal Trust*
- *Data Routing*

3.4.1 Active Detection Routing

A track detects a path without data packings that is intended to convince the opponent to initiate an attack in order to define the action of the attack and then mark the position of the black hole. The system therefore reduces the trust of

suspect nodes and increases the confidence of nodes in successful routes. Via active detection, nodal trust can be quickly gained and the data route can be effectively selected to escape black troubles. The source node selects an undetected neighbor node at random in this scheme to establish an active detection path. In view of the fact that the longest detection route is w , the detection route reduces its duration by 1 per hop up to 0, which then ends. This section describes how the active detection routing protocol is implemented. As shown in Figure 2 the content can be divided into 6 sections of the detection routing packet: (b) the source node identification; (d) the maximum route length of the detection route; (e) the recognition that each of the wops is backed to the source; and (f) the packet identification.

head	type	source	w	ω	id
------	------	--------	-----	----------	----

To start the detection process, the source node selects an undetected node. The overall route length is reduced by 1 until the detection packet receives nodes. If 0 is then generate a feedback packet, start a feedback path to the source and restore the initial value. If not 0, the next hop is selected as well; otherwise the path is terminated. The feedback package is structured and comprises six parts: (a) the header of a packet; (b) the type of packet; (c) the source node ID; (d) the destination node;

head	type	source	Destination	S-id	id
------	------	--------	-------------	------	----

The feedback packet is routed back to the data source; because nodes cache the detection route info, the feedback packet is able to return back to the source, and the following is the algorithm for the detection route protocol.

3.4.2 Nodal Trust

During data routing and detection routing, every node will perform a nodal trust calculation to aid in black hole avoidance. When node A performs a detection route for node B at time t , if the detection data are successfully routed.

$$\{\Delta_A^B(t_1) | \Lambda_A^B(t_1), \Delta_A^B(t_2) | \Lambda_A^B(t_2), \dots, \Delta_A^B(t_w) | \Lambda_A^B(t_w)\}$$

Then, during period t , the total direction trust of A to B is:

$$C_A^B = \begin{cases} \sum_{i=1}^w \{(\Delta_A^B(t_i) | \Lambda_A^B(t_i)) \cdot \bar{h}(i)\} & w \neq 0 \\ 0 & w = 0 \end{cases}$$

Nodal direction trust: Consider the trust set of node A to node B during t to be:

Nodal recommendation trust: Node A is the trust evaluator, node C is the target of evaluation, and node B is a recommender of A. Consider $B \rightarrow A \rightarrow C$ to be the direction trust of A to B and $C \rightarrow B \rightarrow C$ to be the direction trust of B to C; then, the recommendation trust of A to C is

$$R_A^C = C_A^B \times C_B^C$$

For the trust of multiple recommendations, the calculation of the recommendation trust from A to B, B to C, etc., until D to E is

$$R_A^E = C_A^B \times C_B^C \times C_C^D \times C_D^E$$

Recommendation trust merging: Consider that the recommender set of node A is AR , $in \in AR$ and that the recommendation trust of in to node K is $R_{in}^{A,K}$; then, the merged trust of A to K is

$$U_A^K = \sum_{n_i \in A_n} (u_{n_i} R_{n_i}^{A,K}) \quad | u_{n_i} = \frac{R_A^{n_i,K}}{(R_A^{n_1,K} + R_A^{n_2,K} + \dots + R_A^{n_{m-1},K} + R_A^{n_m,K})}$$

Comprehensive trust: Comprehensive trust is the total trust, which merges the recommendation trust and direction trust:

The comprehensive trust of a node can be computed as follows. After the node launches a detection route, it calculates the direction trust according to Eq.

For each received feedback packet. Through interactions, the node obtains the recommendation trust from its neighbors according to T_{ij} , and it then calculates the merged trust according to Eq. (1) for the multiple-recommendation trust. Finally, it calculates the comprehensive trust according to Eq. (2).

3.4.3 Data Routing

The data routing refers to the process of nodal data routing to the sink. The routing protocol is similar to common routing protocols in WSNs; the difference is that the route will select a node with high trust for the next hop to avoid black holes and thus improve the success ratio of reaching the sink.

The central principle of data routing is to pick a node from the group of applicants closer to the sink, whose trust is greater than the predefined threshold as the next hop when a data packet is received. If the node does not find such the right next hop node, the upper node receives a feedback failure, and the upper node recalculates the unselected node set and selects the node with the highest confidence as the second hop; likewise, when it can't find the next hop, the upper node will forward a feedback failure to the upper node. The top node, which works the same way, will pick another node from its neighbors near the platform before data is redirected to the platform or there is no way to the platform.

Algorithm 1: Active Detection Routing Protocol

```
1: Initialization
2: For each neighbor node  $A_n$  Do
3:   Let  $A_n$ .accessTime=Current_time
4: End for
5: For each node that generates a detection packet, such as node A, Do
6:   Construct packet P, and do value assignment for  $\varnothing$  and  $\varnothing'$ 
7:   Select B as the next hop which B meets access time is the minimum and
   nearer the sink
   //B is the node that is the longest time undetected and nearer the sink
8:   Send packet P to node B
9: End for
10: For each node that receives a detection packet, such as node B, Do
11:   let  $P.\varnothing = P.\varnothing - 1$ ,  $P.\varnothing' = P.\varnothing' - 1$ 
12:   If  $\varnothing' = 0$  then
13:     Construct feedback packet q, and do value assignment for each part
14:     Send feedback packet q to the source
15:   End if
16:   If  $P.\varnothing \neq 0$  then
17:     detection routing continue
18:   End if
19: End for
20: For each node that receives feedback packet q, such as node C, Do
21:   If q.destination is not itself then
22:     send q to the source node
23:   End if
24: End for
```

Algorithm 2: Data Routing Protocol

```
1: For each node that generates or receives a data packet, such as node A, Do
2:   select B as the next hop such that B has never been selected in this data
   routing process, has the largest trust and is nearer the sink
3:   If A finds such node, for instance, node B
4:     Send data packet P to node B
5:     If node B is the sink then
6:       this data routing procession is completed
7:     End if
8:   Else
9:     Send failure feedback to the upper node, such as node C
10:   End if
11: End for
12: For each node that receives failure feedback, such as node B, Do
13:   Repeat step 2 to step 11
14: End for
```

CHAPTER 4

SOFTWARE SPECIFICATION

14

4.1 SYSTEM REQUIREMENTS

4.1.1 HARDWARE REQUIREMENTS

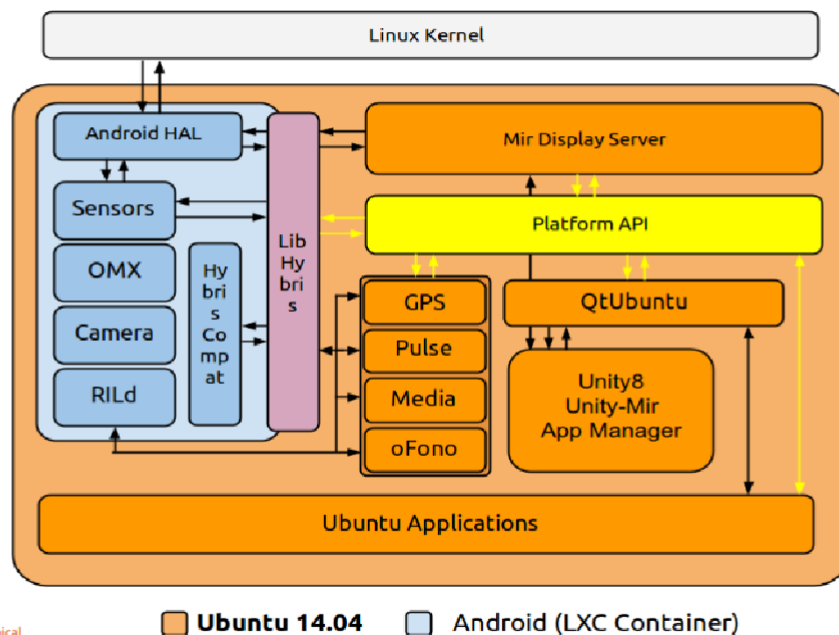
❖ Processor	:	Intel Pentium IV
❖ Processor Speed	:	1.4 GHz
❖ Memory (RAM)	:	Default
❖ Hard disk	:	Default
❖ Monitor	:	Default
❖ Input Device	:	Keyboard (104)

4.1.2 SOFTWARE REQUIREMENTS

❖ Operating System	:	Ubuntu 10.04
❖ Simulator Tool	:	NS 2.34
❖ Language	:	TCL
❖ Protocol Design	:	C++
❖ Platform	:	Independent

4.1.3 INTRODUCTION TO UBUNTU

Ubuntu is a Debian-based Linux operating system, with Unity as its default desktop environment. It is based on free software and named after the Southern African philosophy of Ubuntu (literally, "human-ness"), which often is translated as "humanity towards others" or "the belief in a universal bond of sharing that connects all humanity". According to some metrics, Ubuntu is the most popular Linux distribution.



4.1.3 Architecture Design Ubuntu

4.1.2 BENEFITS OF UBUNTU

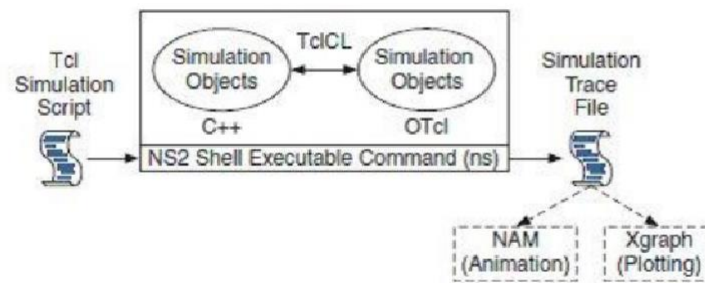
- ❖ Low cost
- ❖ Performance
- ❖ Flexibility
- ❖ Compatibility
- ❖ Choice
- ❖ Fast and easy installation
- ❖ Multitasking
- ❖ Security
- ❖ Open Source

4.1.3 TCL LANGUAGE

8

TCL (Tool Command Language) is a scripting language created by "John Ousterhout". Originally "born out of frustration", according to the author, with programmers devising their own languages intended to be embedded into applications, TCL

gained acceptance on its own. It is commonly used for rapid prototyping, scripted applications, GUIs and testing. TCL is used on embedded systems platforms, both in its full form and in several other small-footprint versions.



Basic architecture of NS.

Figure 4.1.2 Tool Command language

The features of TCL are:

- ❖ Everything can be dynamically redefined and overridden.
- ❖ All data types can be manipulated as strings, including source code.
- ❖ Event-driven interface to sockets and files. Time-based and user-defined events are also possible.
- ❖ All commands defined by TCL itself generate error messages on incorrect usage.
- ❖ Extensibility, via C, C++, Java, and TCL
- ❖ Interpreted language using byte code
- ❖ Full Unicode support, first released 1999
- ❖ Cross-platform: Windows API, Unix, Linux, Macintosh, etc.
- ❖ Close integration with windowing (GUI) interface
- ❖ Multiple distribution mechanisms exist:
- ❖ Full development version (e.g., Active State TCL)

NS2 consists mainly of two languages. C++ and OTCL. Each of these two languages has its own strengths and weaknesses. NS2 beautifully integrates these two languages to draw out their strengths.

LINK

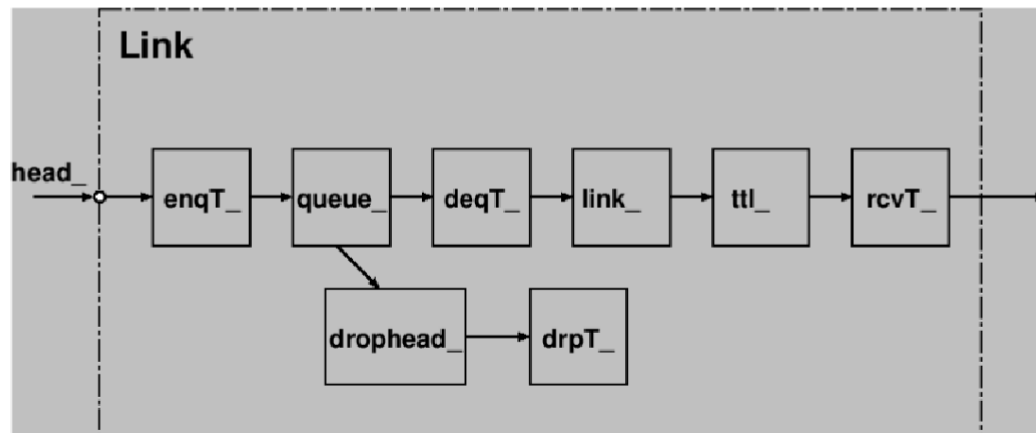


Figure 4.1.3 Link

Another important compound object in NS is a link. If a user creates a connection using a Simulator Object duplex link feature, two simple links are formed in both directions. One thing that needs to be noted is that a node output queue is actually used in a simple connection entity. Delay object which simulates the delay in links and packets dropped in queues are sent to a zero agent and freed there. Finally, for every packet received, the TTL object calculates the time to live parameters and updates the packet TTL area.

STARTING NS

NS starts with the command `ns` (assuming that we are in the directory with the `ns` executable, or that `where` path points to that directory), `where` is the name of a TCL script file which defines the simulation scenario (i.e. the topology and the events).

We could also just start `ns` without any arguments and enter the TCL commands in the TCL shell, but that is definitely less comfortable. Everything else depends on the TCL script.

PROTOCOLS

Wireless networks have different routing protocols. DSR, AODV and DSDV are the most common. This study attempts to compare these three protocols in the various environments on a performance basis. The NS2 is the main simulator, the NAM and Trace Graph used to make the plot from the trace files. The Simulation Tools are NS2. The results of the study clearly show that in different settings the various protocols act differently. The findings also highlight the essential features of various protocols based on their effectiveness and thus recommend improved protocols. Names of the protocol: WSN, AODV, D SR, DSDV, NS2.

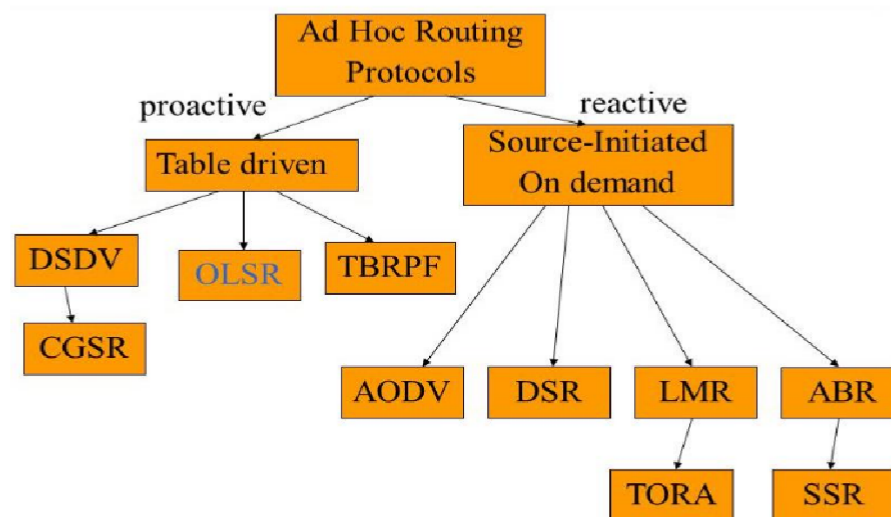


Figure4.1.4. Protocols

ROUTING ALGORITHMS

Most QoS routing algorithms represent an extension of existing classic best-effort routing algorithms. These algorithms can be classified into two different categories: on-demand (reactive) such as DSR, AODV, and TORA, and table-driven (proactive) such as Destination Sequenced Distance Vector protocol (DSDV). In the on-demand protocols, routes are discovered between a source and a destination only when the need arises to send data. This provides a reduced overhead of communication and scalability.

21 DYNAMIC SOURCE ROUTING PROTOCOL (DSR)

DSR is one of the most popular ad hoc wireless network routing algorithms. It was built by Johnson, Maltz and Broch originally. DSR uses source routing that enables loop-free packet routing. The efficiency is increased by the use of promiscuous listening mode to cache routing information for future use, either through transmission of route discovery requests or by overhearing packets. The routing protocol is easy and effective for ad-hoc networks. It is divided into two major stages: road detection and road maintenance.

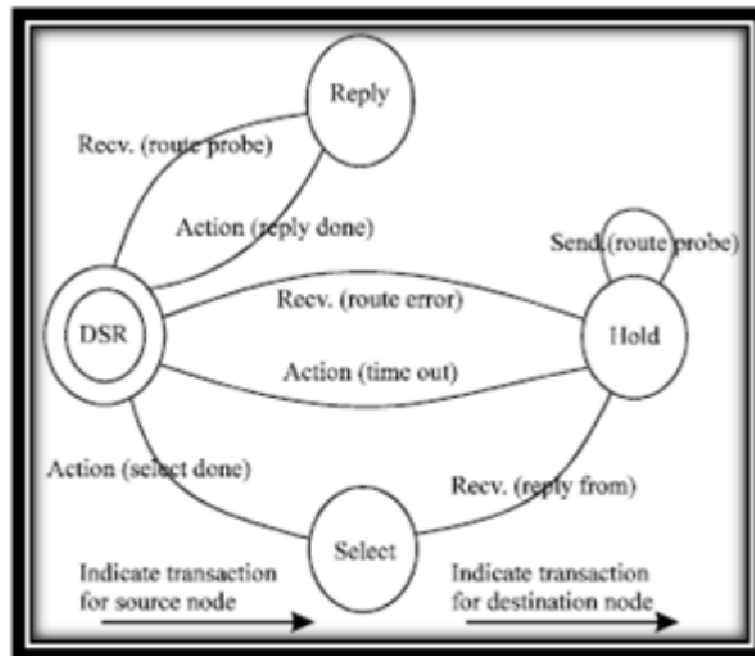


Figure 4.1.5 DSR Protocol

THE ADHOC ON DEMAND DISTANCE-VECTOR PROTOCOL

AODV is an additional ad-hoc network routing algorithm. In contrast to DSR, the source routing is not available, but is on-demand like DSR. In AODV the routing table used for storing destination and next hop IP addresses and destination sequence numbers is held in each node. The destination address of any entry in the routing table is next hop, the list of nodes of precursors, life and distance.

Interesting concepts of ADOV

Features

18

- ❖ Because of its reactive nature, AODV can handle highly dynamic behavior of Vehicle Ad-hoc networks.
- ❖ Used for both unicasts and multicasts using the 'J' (Join multicast group) flag in the packets.

Limitations

- ❖ Requirement on broadcast medium: The algorithm expects/requires that the nodes in the broadcast medium can detect each other's broadcasts.
- ❖ No reuse of routing info: AODV lacks an efficient route maintenance technique. The routing info is always obtained on demand, including for common case traffic.
- ❖ It is vulnerable to misuse: The messages can be misused for insider attacks including route disruption, route invasion, node isolation, and consumption.
- ❖ High route discovery latency: AODV is a reactive routing protocol. This means that AODV does not discover route until a flow is initiated.

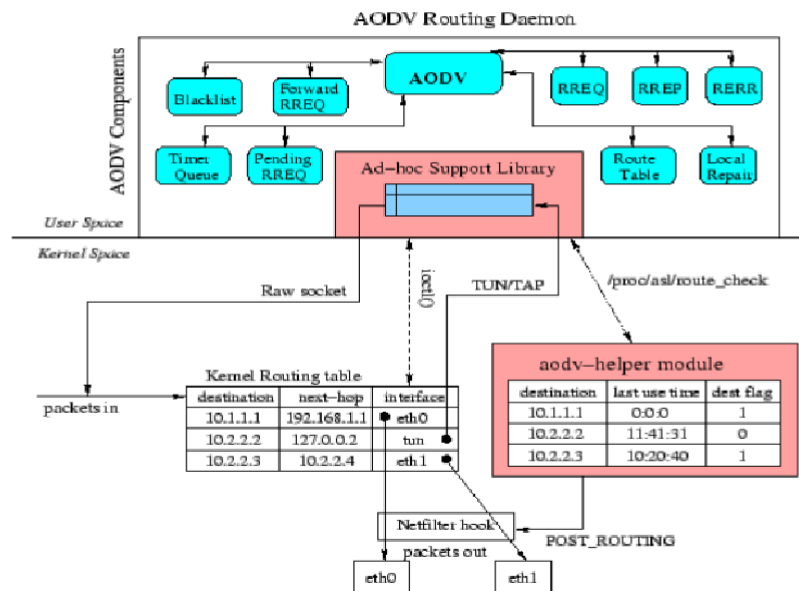


Figure 4.1.6 AODV Routing Protocol

DSDV - THE DESTINATION SEQUENCED DISTANCE VECTOR PROTOCOL

DSDV is one of the most popular routing algorithms for WSN table-driven systems. It's a protocol for the distance vector. The sequence of hops selected in this way leads to x along the shortest path. Each node tracks the cost of its outgoing links and regularly transmits its current estimate of its shortest distance to every other node in the network for the purpose of keeping distance forecasts up-to-date.

Advantages

- ❖ Count to infinity problem is reduced in DSDV. We can avoid extra traffic with incremental updates instead of full dump updates.
- ❖ Path Selection: DSDV maintains only the best path instead of maintaining multiple paths to every destination.

THE ADVANTAGES OF NETWORKING

Networks allow computers, and hence their users, to be connected together. They also allow for the easy sharing of information and resources, and cooperation between the devices in other ways. Some of the major benefits as follows.

❖ Connectivity and Communication

Networks connect computers and the users of those computers. Individuals within a building or work group can be connected into LAN.

❖ Data Sharing

One of the most important uses of networking is to ²²allow the sharing of data. True networking allows thousands of employees to share data much more easily and quickly.

❖ Hardware Sharing

Networks facilitate the sharing of hardware devices. For example, instead of giving each of 10 employees in a department an expensive color printer, ²²one printer can be placed on the network for everyone to share.

❖ Rendezvous Access

The Rendezvous is itself an enormous network. The significance of the Rendezvous on mode Rendezvous society is hard to exaggerate, especially for technical fields.

❖ Rendezvous ¹⁵Access Sharing

Small computer networks allow multiple users to share a single Rendezvous connection. Special hardware devices allow the bandwidth of the connection to be easily allocated to various individuals as they need it.

❖ Data Security and Management

In a business environment, a network allows the administrators too much better manage the company's critical data.

4.2.1 INTRODUCTION



Microsystems has added the wireless capabilities to ns-2. NS-2 is available on several platforms such as FreeBSD, Linux, SunOS and Solaris. NS-2 also builds and runs under Windows with Cygwin. Simple scenarios should run on any reasonable machine; however, very large scenarios benefit from large amounts of memory and fast CPU's.

4.2.2 NS-2 LANGUAGE

NS-2 is basically written in C++, with an OTcl (Object Tool Command Language) interpreter as a front-end. It supports a class hierarchy in C++, called compiled hierarchy and a similar one within the OTcl interpreter, called interpreter hierarchy. Some objects are completely implemented in C++, some others in OTcl and some are implemented in both.

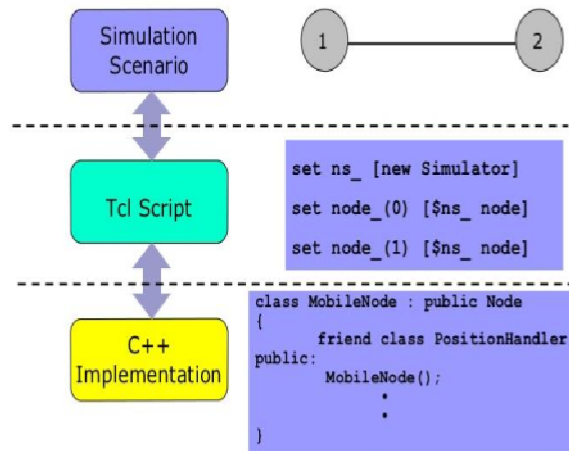


Figure 4.2.2 NS2 language

4.2.3 ARCHITECTURE OF NS-2

As stated, ns-2 is a discrete event simulator directed towards objects. The simulator currently has five schedulers which each have a different data structure to implement: simple connection lists, heap, calendar queue (default) and a special form known as "real-time".

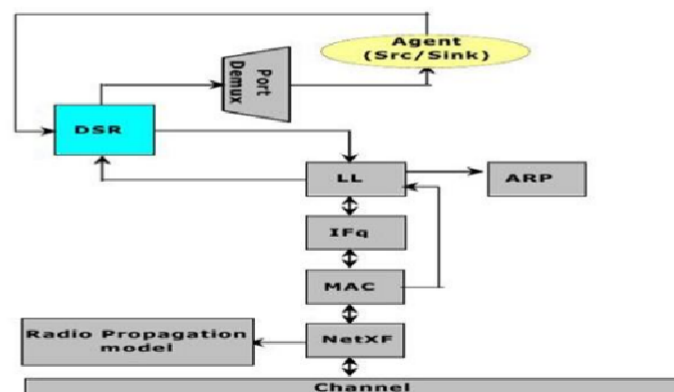
The scheduler runs by selecting the next earliest event, executing it to completion, and returning to execute the next event. The units of time used by the scheduler are seconds.

An event is managed when a handler class is called. NsObject with TclObject as his twin in the OTcl universe is the most effective handler. They offer all the fundamental functions that enable objects to interact. The recipient feature category is primarily used for this purpose. The so-called command function provides for managing OTcl statements in C++ NsObjects. For some essential classes such as the classification system, the connector, and the track file class, NsObject is the parent class.

Physical operations in the ns-2 network are transferred into events, in the order of their scheduled events are queued and processed. And with the processed events, the simulation time advances. And even the simulation "time" cannot be the "input" of real life. But ns-2 can model key network elements, traffic models and applications for what kind of tasks can ns-2 be carried out. It can usually configure transport layer protocols, protocols for routing, interface queues and layer mechanisms for links.

It can easily see that this software tool in fact could provide us a whole view of the network construction, meanwhile, it also maintain the flexibility for us to decide. Thus, just this one software can help us simulate nearly all parts of the network. This definitely will save us great amount of cost invested on network constructing. The following Figure 3 shows a layered structure which ns-2 can simulate for us.

After the simulation finish, the way ns-2 used to present the most details information on that much network layer is that it provides us a huge trace file Line-



by-line documentation of all activities. See therefore now why the process powered by events is used in ns-2 because it could keep track of anything that ever happened. And follow these documents for assessing the performance of network special things such as the protocol for routing, loading of the Mac layer, etc.

4.2.3. NS-2 simulate layered structure of network

The OTcl script does the project by initiating an event scheduler, creates the network topology with the network objects and plumbing functions in the library, and tells traffic sources when to start and stop transmitting packets through the event scheduler, as shown in Figure 4.2.3. For data flow of the simulation one-time ns-2 user input of an OTcl source.

In this view, ns-2 will be treed as an objective-oriented Tcl script transducer (OTcl) with an event programmer and a network-component object library and a network setup module. This OTcl script file will now be passed on to ns-2

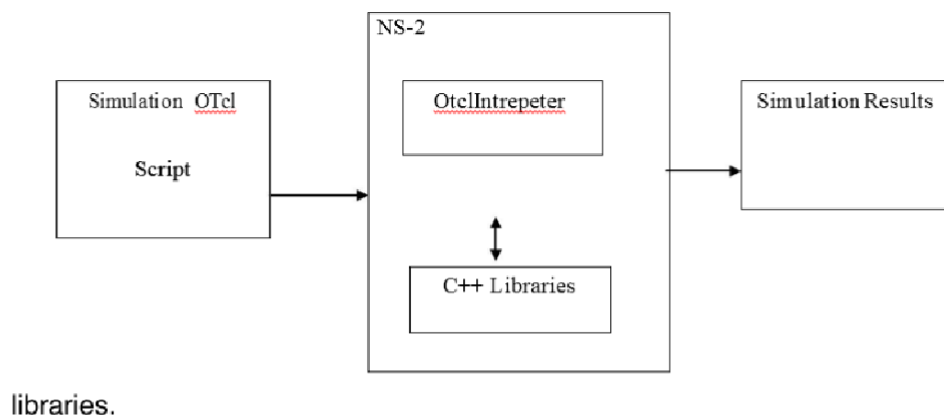


Figure 4.2.4 Data flow for one time simulation

TRACE FILES

Old Wireless Trace File Format

A trace in this format always begins with one of the characters in table 4.1.

This character is succeeded by a white space separated list of values specific for the used protocol and the type of the message.

N	Node Property
I	IP Level Packet Information
H	Next Hop Information
M	Mac Level Packet Information
P	Application Level Packet Information

Table 4.2.5 Flag Types New Wireless Trace Format

4.2.4 MOTIVATION FOR SIMULATIONS

1. Cheap does not require costly equipment
2. Complex scenarios can be easily tested
3. Results can be quickly obtained – more ideas can be tested in a smaller timeframe
4. The real thing isn't yet available
5. Controlled experimental conditions– Repeatability helps aid debugging
6. Disadvantages: Real systems too complex to model

4.2.5 NS FEATURES

- ❖ NS is an object oriented discrete event simulator
 - Simulator maintains list of events and executes one event after another
 - Single thread of control: no locking or race conditions
- ❖ Back end is C++ event scheduler
 - Protocols mostly
 - Fast to run, more control
- ❖ Front end is TCL
 - Creating scenarios, extensions to C++ protocols
 - fast to write and change

4.2.6 NS PROGRAMMING STRUCTURE

- ❖ Create the event scheduler
- ❖ Turn on tracing
- ❖ Create network topology
- ❖ Create transport connections
- ❖ Generate traffic
- ❖ Insert errors

EVENT SCHEDULAR

In this Event scheduler while we processing many data's at a time it will process one by one (i.e.) FIFO concept, so there is no congestion while transferring the packets.

PACKETS

It is the collection of data, whether header is called or not all header files where present in the stack registers.

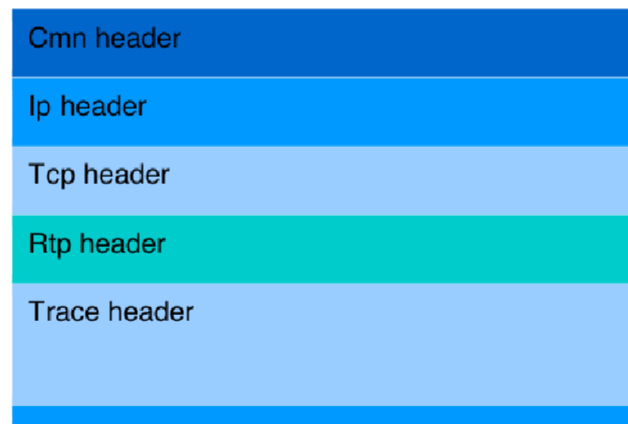


Figure 4.2.6 Event Scheduler

TURN ON TRACING

Trace packets on individual link Trace file format

event	time	from node	to node	pkt type	pkt size	flags	fid	src addr	dst addr	seq num	pkt id
<pre> r : receive (at to_node) + : enqueue (at queue) src_addr : node.port (3.0) - : dequeue (at queue) dst_addr : node.port (0.0) d : drop (at queue) </pre>											
r	1.3556	3	2	ack	40	-----	1	3.0	0.0	15	201
+	1.3556	2	0	ack	40	-----	1	3.0	0.0	15	201
-	1.3556	2	0	ack	40	-----	1	3.0	0.0	15	201
r	1.35576	0	2	tcp	1000	-----	1	0.0	3.0	29	199
+	1.35576	2	3	tcp	1000	-----	1	0.0	3.0	29	199
d	1.35576	2	3	tcp	1000	-----	1	0.0	3.0	29	199
+	1.356	1	2	cbr	1000	-----	2	1.0	3.1	157	207
-	1.356	1	2	cbr	1000	-----	2	1.0	3.1	157	207

Figure 4.2.7 Trace file

CREATE NETWORK TOPOLOGY (PHYSICAL LAYER)

The physical layer of the 7-layer OSI computing networking model is the first and lowest layer. This layer is also referred to as PHY. The Physical Layer includes the fundamental network hardware transfer technologies. It is an essential layer that supports the logical data structures of a network's higher level. Because of the many different features of the available hardware technologies this could be the most complex layer in OSI architecture. The Physical Layer describe how raw bits are transmitted over physical connection linking network nodes instead of logical data packets. The bit stream can be grouped into code words or symbols and transformed into a hardware-borne physical.

TRANSPORT CONNECTION (TRANSPORT LAYER)

Both the TCP/IP, which is the backbone of the INTERNET and the general networking OSI models, have transport layers. These two models have slightly different meanings of the transport layer. This article specifically concerns the TCP/IP model which, in contrast to the defining interface model OSI, TCP is mainly used for a convenient application programming interface to internet hosts. The most popular transportation protocol is (TCP). The whole TCP/IP Internet Protocol Suite was named by the company. It is used for connecting transmissions, while the UDP series for basic messaging transmissions is used. Due to its state

of complete design with secure data transmission and stream services, TCP is the most complex protocol.

GENERATE TRAFFIC (APPLICATION LAYER)

In TCP/IP an application layer is made up of all the protocols and methods used by the Internet Protocol (IP) network for the establishment of underlying host to host connections. In the OSI model, the application layer is defined more narrowly and specifically differentiates additional functionality from the transportation layer on 2 additional levels: session layer and presentation layer. Strict modular feature separation at these layers is given by OSI and protocols for each layer

FEASIBILITY ANALYSIS

All tasks can be accomplished, with limitless resources and time. The system analyst must first examine whether the proposed system would be feasible to the company and determine customer requirements before moving through software development measures. The ³⁷main aim of the feasibility study is to assess the value of solving the problem. The system's effectiveness depends also on how much viability is studied. Many feasibility studies on any system must be carried out.

But there are ³⁷three main feasibility tests to be performed. They are

- ❖ OPERATIONAL FEASIBILITY
- ❖ TECHNICAL FEASIBILITY
- ❖ ECONOMICAL FEASIBILITY

OPERATIONAL FEASIBILITY

Operational feasibility studies are a must during the review of feasibility. Since operational viability or usability should be very high according to software engineering principles. The device is performed and found to be operational.

TECHNICAL FEASIBILITY

The device analyst is responsible for monitoring the technological viability of the proposal. The technical feasibility evaluation shall be carried out in the light of the hardware used for device construction, data storage, processing and performance. The system analyst must check if sufficient resources are available for the program to work smoothly for the organization or consumer who is implementing the system. The standards for this application are actually much lower and are therefore technically feasible.

ECONOMICAL FEASIBILITY

To move on to the implementation of the framework proposed. The system analyst must ensure that the proposed system is cost-effective and that the costs for operating it consist of the cost advantage that the system will provide. The cost for creation of crypto media is not high, since no additional hardware and software are needed. The device is also cost-effective. The system design is the preparation process for a new system to record or replace the existing system completely. The purpose of the design stage is to prepare a solution. The first step from the problem domain to the solution domain is the process. The device architecture is the crucial factor that affects software quality. System design is also known as high-level design. The design process transforms the system's abstract aspects into the system's physical aspects.

Summary

In this study, our implementation tool and its functions and also every step-by-step description of processes were discussed. First, Ubuntu OS, this operating system is a Linux operating system, and here in this operating system we use a network simulator tool. Ubuntu is a Linux operating system based on Debian that uses Unity as its standard desktop environment. It is based on free software, named after Ubuntu (literally 'humanity') Southern Africa ideology, which also translates into 'humanities to all,' or 'the conviction that all mankind have a common bond of sharing.' Second, a scripting language provided by "John Ouster out" is TCL (Tool Command Language). According to the authors, TCL was originally "born out of dissatisfaction" by the design of its own languages for application-inclusion. With this TCL, we also discuss protocols and implementations in the AODV, DSR, DSDV and LINK LAYER network simulator tools. Finally Network Simulator tool (NS2) - Network simulator architecture, ns2 programming structure features, multiple simulator layers, trace files and trace analysis were discussed here. NS2 research. The applications used for implementing NS2 simulation projects are above described in the network simulator tool.

CHAPTER 5

RESULT AND DISCUSSION

PERFROMANCE ANALYSIS

This research used ns-2 to test the efficiency of HEIDS as a network simulator and performed several simulations. The uniform distribution of all sensor nodes is altered. The place of the sink is calculated randomly. This study assesses the routing efficiency in scenarios with different sensor node numbers. The current data indicates that detection accuracy study should have been carried out in this way. Early researchers developed experimental designs which seem to exclude important information types. Following researchers systematically based on earlier designs to create a complete literature in a single basic design around variations. While this literature definitely has advanced knowledge, it may be much smaller than it was. If descriptive studies had begun early, the literature may have made a different and more productive development.

There are also some theoretical consequences of the results. The present data are most clearly inconsistent with the primacy of the presumption of source conduct, which is fundamental to the theory of deception. Theories that render this hypothesis can need to be replenished to prevent or qualify. Network simulator and various simulations for WSN performance assessment.

The key output measurements are evaluated in this research:

- 1) Transmission ratio of packets: the mean sending and receiving rate of the packet is measured then calculating the sending ratio.
- 2) Consumption of energy: Means Reduce network energy consumption, thereby improving the rate of energy performance.
- 3) End-to-end delay: means the time delay of the source node when sending a report on the sink.

CHAPTER 6

CONCLUSION AND FUTURE ENHANCEMENTS

We propose a trust control system that increases the safety of hybrid and efficient intrusion detection systems in networks (HEIDS). Two trust and decision-making systems were used here. The value of confidence is derived from Bayesian inference, and from decision-making based on the principle of Dempster's Shafer, which is mathematical proof theory.

The proposal for a new active detection security and confidence routing scheme, with the excellent features: (1) High probability, safety and scalability of routing successfully. The trust system will easily detect the nodal confidence and then avoid suspicious nodes in order to achieve an effective routing probability of almost 100%. (2) High productivity in energy production. The Trust system uses residual energy in its entirety to create numerous detection routes. The theoretical research and the experimental results demonstrate that our scheme increases the likelihood of effective routing more than 3 times, often up to 10 times.

FUTURE WORK

A technology to be integrated into Trust's approach in future with the energy efficiency sleep wake planning. This will allow us to achieve higher energy efficiency and higher energy usage than the previous Active Trust model.

REFERENCE

- [1] N. Roseveare and B. Natarajan, "A structured approach to optimization of energy harvesting wireless sensor networks", IEEE Consumer Communications and Networking Conference (CCNC), pp. 420-425, Las Vegas, 2013.
- [2] O. Younis, M. Krunz and S. Ramasubramanian, "Node clustering in wireless sensor networks: recent developments and deployment challenges", IEEE Network, Vol. 20, No.3, pp. 20-25, 2006.
- [3] C.E. Perkins, E.M. Royer, "The ad hoc on-demand distance vector protocol", Ad hoc networking, Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA, pp. 173-219, 2001.
- [4] [4] E. Belding-Royer, "Hierarchical routing in ad hoc mobile networks", Wireless Communications and Mobile Computing, Vol.2, No.5, pp. 515-532, 2002.
- [5] M. Lotfinezhad and B. Liang, "Effect of partially correlated data on clustering in wireless sensor networks", Proceedings of the IEEE International Communications Society Conference on Sensor and Ad Hoc Communications and Networks (SECON), Citeseer, pp.172-181, 2004.
- [6] A.A. Abbasi and M. Younis, "A survey on clustering algorithms for wireless sensor networks", Computer Communications, Vol. 30, pp. 2826-2841, 2007.
- [7] W. Heinzelman, A. Chandrakasan and H. Balakrishnan, "Energyefficient communication protocol for wireless microsensor networks", Proceedings of the 33rd Hawaii International Conference on System Sciences, Vol. 8, Citeseer, pp. 802, 2000.
- [8] Gupta, D. Riordan and S. Sampalli, "Cluster-head election using fuzzy logic for wireless sensor networks", Proceedings of the IEEE 3rd Annual

Communication Networks and Services Research Conference, pp. 255-260, 2005.

- [9] Alchihabi, A. Dervis, E. Ever and F. Al-Turjman, "A Generic Framework for Optimizing Performance Metrics by Tuning Parameters of Clustering Protocols in WSNs", Wireless Networks,
- [10] J. Kim, S. Park, Y. Han and T. Chung, "CHEF: cluster head election mechanism using fuzzy logic in wireless sensor networks", Proceedings of the IEEE 10th International Conference on Advanced Communication Technology (ICACT), pp. 654-659, 2008.

A NOVEL ANALYSIS OF HYBRID AND EFFICIENT INTRUSION DETECTION SYSTEMS IN WIRELESS SENSOR NETWORKS

ORIGINALITY REPORT

12%

SIMILARITY INDEX

9%

INTERNET SOURCES

6%

PUBLICATIONS

7%

STUDENT PAPERS

PRIMARY SOURCES

1	creativecommons.org Internet Source	<1%
2	www.igi-global.com Internet Source	<1%
3	www.midland-telecom.com Internet Source	<1%
4	www.uok.ac.in Internet Source	<1%
5	Kai Fan, Wei Wang, Hui Li, Yintang Yang. "Adaptive Sensing Private Property Protection Protocol Based on Cloud", International Journal of Distributed Sensor Networks, 2015 Publication	<1%
6	www.sathyabama.ac.in Internet Source	<1%
7	www.researchscript.com Internet Source	<1%
8	Submitted to University of Glamorgan Student Paper	

<1 %

9

Submitted to Anglia Ruskin University

Student Paper

<1 %

10

Submitted to Harrisburg University of Science and Technology

Student Paper

<1 %

11

www.ijser.org

Internet Source

<1 %

12

Pengliu Tan. "A Hybrid Routing Mechanism for ZigBee Wireless Sensor Networks", Communications in Computer and Information Science, 2011

Publication

<1 %

13

Submitted to Caledonian College of Engineering

Student Paper

<1 %

14

doc.quasardb.net

Internet Source

<1 %

15

Submitted to Newcastle College, Tyne & Wear

Student Paper

<1 %

16

www.ece.ksu.edu

Internet Source

<1 %

17

Submitted to Indian Institute of Technology, Kanpur

Student Paper

<1 %

18	ijiet.com Internet Source	<1 %
19	Submitted to Dublin City University Student Paper	<1 %
20	ns2ultimate.tumblr.com Internet Source	<1 %
21	www.ijeit.com Internet Source	<1 %
22	Submitted to CGA–Certified General Accountants Association of Canada Student Paper	<1 %
23	osiris.sunderland.ac.uk Internet Source	<1 %
24	www.emerald.com Internet Source	<1 %
25	imraan-prrec.blogspot.com Internet Source	<1 %
26	www.citeulike.org Internet Source	<1 %
27	zenodo.org Internet Source	<1 %
28	P. Goswami, A. D. Jadhav. "Evaluating the performance of routing protocols in Wireless Sensor Networks", 2012 Third International Conference on Computing, Communication	<1 %

and Networking Technologies (ICCCNT'12), 2012

Publication

29

"" , IEEE Network, 5/2006

Publication

<1 %

30

Submitted to Gulf University

Student Paper

<1 %

31

Submitted to University of Missouri, Kansas
City

Student Paper

<1 %

32

citlprojects.com

Internet Source

<1 %

33

www.haystack.tv

Internet Source

<1 %

34

text-id.123dok.com

Internet Source

<1 %

35

www.deepdyve.com

Internet Source

<1 %

36

Giovanni Bucci, Edoardo Fiorucci, Carmine
Landi. "Industrial Measurement and Control",
Wiley, 1999

Publication

<1 %

37

www.ijarcce.com

Internet Source

<1 %

38

G. Karthiga, C. Preethi, R. Delshi Howsalya Devi. "Localization in wireless sensor network based on mobile anchor and chord selection", 2014 International Conference on Communication and Network Technologies, 2014

Publication

<1 %

39

Rahman, M.A.. "Network modelling and simulation tools", Simulation Modelling Practice and Theory, 200907

Publication

<1 %

40

portal.research.lu.se

Internet Source

<1 %

41

link.springer.com

Internet Source

<1 %

Exclude quotes On

Exclude matches < 20 words

Exclude bibliography On