Energy Efficient Location Privacy Preserving Based Qos Improvement in Wireless Multimedia Sensor Network

R.Kiruthika, L.Devi

Abstract— To introduce an Energy Efficient Location Privacy Preserving (EELPP) Protocol for WMSNs that is based on the Location Aided Routing (LAR) it's mainly used in to improve QoS in network. LAR makes significant reduction in the energy consumption of the nodes batteries by limiting the area of discovering a new route to a smaller zone. Thus, control packets overhead are significantly reduced. In EELPP a reference wireless base station is used and the network's circular area centered at the base station is divided into six equal sub-areas.At route discovery instead of flooding control packets to the whole network area, they are flooded to only the sub-area of the destination mobile node. The base station stores locations of the nodes in a position table. To show the efficiency of the proposed protocol we present simulations using NS-2. Simulation results show that EELAR protocol makes an improvement in control packet overhead and delivery ratio compared to AODV. To reduce the energy cost, nodes are active only during data transmission and the intersection of node creates a larger merged node, to reduce the number of fake packets and also boost privacy preservation. Simulation and analytical results demonstrate that our scheme can provide stronger privacy protection than routing-based schemes and requires much less energy than data preventing based.

Index Terms— WSN, Multimedia, Qos, Image recognition, Security, Network, Node.

1 Introduction

The security threats can usually be classified into: content security and contextual security. For the content security threat, the adversary attempts to observe the content of the packets sent in the network to learn the sensed data and the identities and locations of the source nodes. This security threat can be countered by encrypting the packets' contents and using pseudonyms instead of the real identities. For the contextual security threat, the adversary eavesdrops on the network transmissions and uses traffic analysis techniques to deduce sensitive information, including whether, when, and where the data are collected. Actually, the act of packet transmission itself reveals information even if the packets are strongly encrypted and the adversary could not interpret them.

The existing source location security-preserving schemes can be classified into global-adversary-based and routing-based schemes. These schemes employ either weak or unrealistic adversary model. The global-adversary-based schemes, assume that the adversary can monitor every radio transmission in every communication link in the network. To preserve source nodes' location security, each node has to send packets periodically, e.g., at fixed time slots.

R.Kiruthika *working as an Assistant Professor in the Department of Computer Science at Muthayammal College of Arts & Science, Namakkal, India*

L.Devi *working as an Associate Professor in the Department of Computer Science at Muthayammal College of Arts & Science, Namakkal, India*

If a node does not have sensed data at one time slot, it sends dummy packet, so that the adversary cannot know whether the packet is for a real event or dummy data. However, the assumption that the adversary can monitor the transmissions of the entire network is not realistic, especially when the WRN is deployed in a large area. Moreover, if the adversary has a global view to the network traffic, he can locate pandas without making use of the network transmissions. Transmitting dummy packets periodically consumes a significant amount of energy and bandwidth, and decreases packet delivery ratio due to increasing packet collision, which makes these schemes impractical for WRNs with limited-energy nodes.

On the contrary, routing-based schemes use weak adversary model assuming that the adversary has limited overhearing capability, e.g., similar to a relay node's transmission range, and can monitor only one local area at a time. These schemes assume that the adversary starts from the Sink and tries to locate the origin of a transmission by back tracing the hop-by-hop movement of the packets sent from the source node. Once the adversary overhears a transmission made from node A, he moves to A and waits. Then, he overhears a transmission from node B and moves to B to be closer to the source node, and so on until he locates the source node. Routing-based schemes try to preserve source nodes' location security by sending packets through different routes instead of one route, to make it infeasible for adversaries to trace back packets from the Sink to the source node because they cannot receive a continuous flow of packets. However, if the adversary's overhearing range is larger than the relay nodes' transmission range, the likelihood of capturing a large ratio of the packets sent from a source node significantly increases. It is shown that if the adversary's overhearing range is three times the relay nodes' transmission range, the likelihood of locating pandas is as high as 0.97. Moreover, if pandas stay for some time in one location, the adversary may capture enough number of packets to locate the pandas even if the packets are sent through different routes.

1.1 Neighbor set coverage and coverage conditions

We propose a simple distributed heuristic approach to determine a small connected dominating set used as the forward node set. Two approaches can be adopted: In the static approach, a connected dominating set is constructed based on the network topology, but irrelative to any broadcasting. In the dynamic approach, a connected dominating set is constructed for a particular broadcast request, and it is dependent on the location of the source and the progress of the broadcast process. We assume that in the dynamic approach, each node determines its status "on-the-fly" when the broadcast packet arrives at the node. We also assume that the broadcast packet that arrives at v carries information of h most recently visited Nodes for a small h and the corresponding node set is denoted as D (v). This assumption does not lose any generality, since we can assume h to be packet does not carry any routing history information.

1.2 **Neighborhood information**

To address the location security issue, location k-anonymity and cloaking granularity are two commonly used security metrics. A mobile user is considered location k-anonymous if and only if the location information sent to the service provider is made indistinguishable from that of at least k _ 1 other user. To achieve location k-anonymity, exact user locations are extended to cloaked regions such that each region covers at least k users. It requires the area of cloaked region to be larger than a user-specified threshold. While the location k-anonymity protects the user identity (out of k users), it may not be able to prevent the location disclosure (e.g., a cloaked region covering k users in populated areas could be very small). On the other hand, the cloaking granularity prevents the location disclosure but cannot defend against attacks for user identifies in the cases where user locations are publicly known and there is only one user in the cloaked region.

Most of the existing security-aware algorithms, which comply with location k-anonymity model, are concerned with snapshot user locations only. They have not considered the effect of continuous location updates. This may result in serious security breaches when different one-shot queries are frequently issued by a mobile user.3 If an attacker (e.g., the service provider) can collect the historical cloaked regions of a user as well as the mobility pattern (e.g., speed limit), the location security of the user might be compromised. Continuing with the above example, Alice gets the address of the hospital; and at some time on the way to the hospital, Alice wants to gas up her car.

Location-dependent attacks have been studied in some previous works. However, the prior solutions in only considered the cloaking granularity as the security metric, which, as discussed earlier, may fail to protect the user identity in case there is only one user in the cloaked region. Thus, in this paper, we adopt both the cloaking granularity and location k-anonymity as security metrics. We propose a new location cloaking algorithm, called CliqueCloak, to incorporate the effect of continuous location updates in the process of location cloaking. As illustrated in Fig. 2, at time tiþ1, the cloaking algorithm is aware of Rate and MMBA; it; tiþ1, and attempts to find the

We use a graph model to formulate this problem. Each location-based query request is represented by a node in the graph; an edge exists between two nodes only if they are within the MMB of each other and can be potentially cloaked together. To meet the location k-anonymity requirement, the problem becomes to find k-node cliques in the graph such that all the nodes within a clique form a cloaking set. To reduce the computational complexity, we propose to maintain the maximal cliques incrementally. That is, all maximal cliques are identified at the beginning of the process; they are then incrementally maintained based on three classes: positive candidates, negative candidates, and non candidates. Thus, a qualified clique can be quickly identified and used to generate the cloaked region when a new request arrives.

Location-based services (LBSs) provide personalized service to Smartphone/tablet users by exploiting their location information. As smart phones become increasingly popular and resource-rich, LBSs have become more feature rich and versatile, improving users' daily lives by, for example, finding restaurants with their favorite menus, obtaining just-in-time coupons from nearby shopping centers, and tracking their physical fitness.

This problem has received considerable attention from users/consumers, service providers, and government organizations. From the consumers' side, according to a recent survey commissioned by Microsoft, LBS users are concerned about the use of their location information and would like to have control over such information. As for service providers, they also have strong incentives to eliminate or mitigate users' security concerns because LBSs cannot be successfully marketed unless users are comfortable about using them. Finally, the U.S. Department of Commerce recommended, in December 2010, the inclusion of security protection associated with LBSs in electronic security laws in order to provide stronger protection enforcement with legislation support.

In this paper, we formulate the above security problem. We analytically develop inference strategies that the adversary may use to maximize its effectiveness in identifying one or more victims under different system assumptions. We show how the adversary can gainfully incorporate general world knowledge—in the form of a movement model accounting for global movement constraints and preferences—in its inference strategies. We also quantify experimentally the loss of victim nodes' security (possibly as a process over time) as a function of several important system parameters, including the nodal mobility, the inference strategies of the adversaries, and any noise that may appear in the traces or side information (due to either the application of cloaking techniques or inherently imprecise observations). Our contributions are twofold.

We provide extensive analysis both theoretically and experimentally to demonstrate that with the current practice of capturing and publishing anonymous location traces of real users, the concern exists that an adversary could identify the traces of one or more victims in the published data with high probability by invoking a small amount of side information about the participants. In particular, we present comprehensive attack strategies available to the adversary when it collects information about a victim's movement either through direct observations or indirect information sources and show that these attacks are effective in breaching security. We also provide a mathematical framework to show the optimality of specific attack strategies in that they utilize all the available information in the most effective way.

Source-location security (SLP) is an important security issue. Lack of SLP can expose significant information about the traffic carried on the network and the physical world entities. While confidentiality of the message can be ensured through content encryption, it is much more difficult to adequately address the SLP. Preserving SLP is even more challenging in WRNs since the relay nodes consist of only low-cost and low-power radio devices, and are designed tooperate unattended for long periods of time.

So far, few location systems have considered security as an initial design criterion. The Cricket location system6 is a notable exception: location data is delivered to a personal digital assistant under the sole control of the user. Commercial wide-area location-based services will initially appear in mobile cellular systems such as GSM. Texaco's Erica system delivers sensitive customer information to third-party applications. Erica provides an API for third-party software to access customer billing information, micropayment systems, customer preferences, and location information. In this context, individual security becomes much more of a concern. Users of location-aware applications in this scenario could potentially have all their daily movements traced. In a work-in-progress Internet draft that appeared after we submitted this article for publication, Jorge R. Cuellar and colleagues also explore location security in the context of mobile cellular systems.As we do, they suggest using pseudonyms to protect location security. Unlike us, however, they focus on policies and rules they do not consider attacks that might break the unlink ability that pseudonyms offer.

1.3 Network Mixing Ring

We first propose some criteria to quantitatively measure source-location information leakage for routing-based SLP schemes. Through the proposed measurement criteria, we are able to identify security vulnerabilities of some exiting SLP schemes. We then propose a scheme that can provide both content confidentiality and SLP through a two-phase routing. In the first outing phase, the message source randomly selects an intermediate node in the relay domain and then transmits the message to the randomly selected intermediate node (RSIN). This phase provides SLP with a high local degree. In the second routing phase, the messages will be routed to a ring node where the messages will be blended through a network mixing ring (NMR). By integrating the NMR, we can dramatically decrease the local degree and increase the SLP. Our simulation results demonstrate that the proposed scheme is very efficient and can achieve a high message delivery ratio. We believe it can be used in many practical applications.

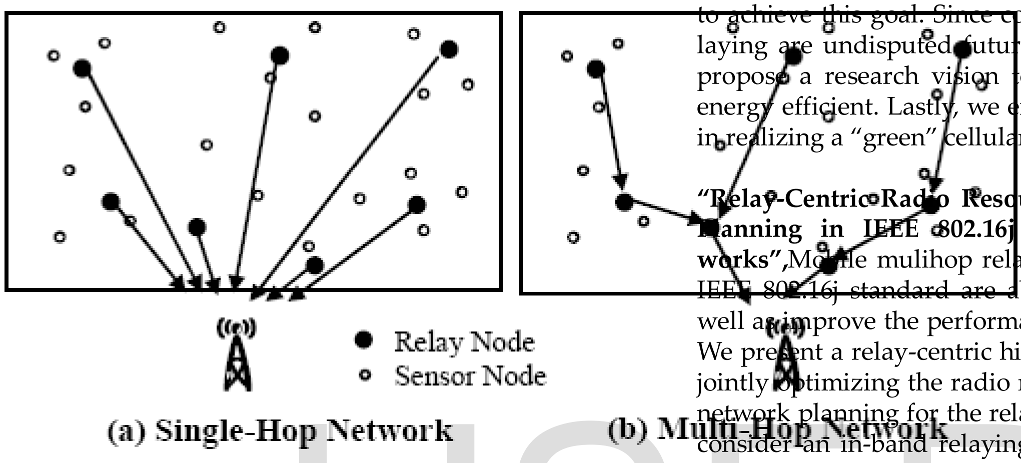
We focus on defining the management of information release and the nature of the security rules and a preference used to control this release, but does not address these issues. Hence could use a subset of our system's rule sets and overall policy architecture as the "security-enabling information"1 stored in a location object proposed coupling of dataand security metadata offers greater accountability than our system when location information has been passed between multiple applications. The practicality of such a system has yet to be determined, however.

After more than two decades of hype, computing and communication technologies are finally converging. Java enabled cell phones run a host of powerful applications including mobile Internet access, while many notebook computers offer high-speed wireless connectivity as a standard feature. The big decision when purchasing a PDA this holiday season is whether to get integrated cellular service or Wi-Fi capability. Location-based services are emerging as the next killer app in personal wireless devices, but there are few safeguards on location security. In fact, the demand for improved public safety is pushing regulation in the opposite direction. Today, when a person reports an emergency from a landline phone by dialing 911 in the United States or 112 in Europe, the system displays the caller's phone number and address to the dispatcher. The US Federal Communications Commission has mandated that, by December 2005, all cellular carriers be able to identify the location of emergency callers using mobile phones to within 50 to 100 meters. In July 2003, the European Commission recommended rapid deployment of a similar location-enhanced 112 service. However, how cellular carriers and other businesses will use this capability remains open to question.

SLP is a key security requirement for military and many civilian applications. In the asset monitoring model, WRNs can be used to monitor the activities or presence of animals in a wild animal habitat. However, the information should be kept unavailable to illegal hunters. In military intelligence networks, to protect the message source, both the message source and the routing path have to be protected from adversarial attacks. Before we describe our proposed SLP scheme in WRNs, we will introduce the system model and adversarial model in this section to capture the relevant features of WRNs and the potential adversaries in SLP applications.

2. Literature Survey

“Relay Node Deployment Strategies in Heterogeneous Wireless Relay Networks: Multiple-Hop Communication Case”, While a lot of existing research attempts to extend the lifetime of a wireless relay network (WRN) by designing energy efficient networking protocols, the impact of random device deployment on system lifetime is not stressed enough. Some research efforts have tried to optimize device deployment with respect to lifetime by assuming devices can be placed deliberately. However, the methodologies and solutions therein are not applicable to a randomly deployed large scale WRN. In



(a) Single-Hop Network (b) Multi-Hop Network

“Fundamental Tradeoffs on Green Wireless Networks”, Traditional design of mobile wireless networks mainly focuses on ubiquitous access and large capacity. However, as energy saving and environmental protection become a global demand and inevitable trend, wireless researchers and engineers need to shift their focus to energy-efficiency oriented design, that is, green radio. In this paper, we propose a framework for green radio research and integrate the fundamental issues that are currently scattered. The skeleton of the framework consists of four fundamental tradeoffs: deployment efficiency - energy efficiency tradeoff, spectrum efficiency - energy efficiency tradeoff, bandwidth - power tradeoff, and delay - power tradeoff. With the help of the four fundamental tradeoffs, we demonstrate that key network performance/cost indicators are all stringed together.The next generation wireless networks are expected to provide high speed internet access anywhere and anytime. The popularity of phone and other types of smart phones doubtlessly accelerates the process and creates new traffic demand, such as mobile video and gaming. The exponentially growing data traffic and the requirement of ubiquitous access have triggered dramatic expansion of network infrastructures and fast escalation of energy demand [3]. Hence, it becomes an urgent need for mobile operators to maintain sustainable capacity growth and, at the same time, limit the electricity bill.

“Green Cellular Networks: A Survey, Some Research Issues and Challenges”, Energy efficiency in cellular networks is a growing concern for cellular operators to not only maintain profitability, but also to reduce the overall environment effects. This emerging trend of achieving energy efficiency in cellular networks is motivating the standardization authorities and network operators to continuously explore future technologies in order to bring improvements in the entire network infrastructure. In this article, we present a brief survey of methods to improve the power efficiency of cellular networks, explore some research issues and Challenges and suggest some techniques to enable an energy efficient or “green” cellular network. Since base stations consume a maximum portion of the total energy used in a cellular system, we will first provide a comprehensive survey on techniques to obtain energy savings in base stations. Next, we discuss how heterogeneous network deployment based on micro, pico and femtocells can be used to achieve this goal. Since cognitive radio and cooperative relaying are undisputed future technologies in this regard, we propose a research vision to make these technologies more energy efficient. Lastly, we explore some broader perspectives in realizing a “green” cellular network technology [4].

“Relay-Centric Radio Resource Management and Network Planning in IEEE 802.16j Mobile Multihop Relay Networks”,Mobile mulihop relay (MMR) networks based on the IEEE 802.16j standard are able to extend the service area as well as improve the performance of mobile WiMAX networks. We present a relay-centric hierarchical optimization model for jointly optimizing the radio resource management (RRM) and network planning for the relay stations in MMR networks. We consider an in-band relaying system. For a relay station, the RRM problem deals with optimizing the amount of bandwidth reserved from the base station and admission control for the mobile subscriber stations (MSSs) using relay-based transmissions so that the utility of a relay station is maximized. A Markov decision process (MDP) model is formulated to obtain the short-term optimal action of a relay station. Based on the optimal action of each relay station, the network planning problem is solved for a group of relay stations by optimizing the relay placement and base station selection over a longer period of time considering uncertainties in user mobility and traffic load in the network. A chance-constrained assignment problem (CCAP) is formulated to obtain the optimal decisions to maximize the total utility of relay stations under the probabilistic constraint on the total bandwidth usage of the base stations. Numerical results show that the proposed scheme outperforms a static scheme. The proposed radio resource management and network planning framework will be useful for design and optimization of Multihop cellular wireless networks in general [7].

3. Problem Statement

In our existing system to used incentive-driven and privacy-preserving systems for large scale message dissemination in mobile networks. To distribute incentives which encourage forwarding behaviors, such as monetary rewards, we want to keep track of the forwarder list. We rely on a Probabilistic one-ownership forwarding algorithm to record the list, so that the exchanged messages can be kept short and privacy-preserving. More specifically, only one hop of forwarder information, instead of the complete list, is recorded, and the information is updated probabilistically following two ownership flipping models, namely, One-Flip and Always-Flip models. We also use a Bluetooth Service Discovery Protocol (SDP) toolkit to enable fast, configuration-free message exchange. Throughout the paper, we use coupon as a typical type of message to illustrate the core ideas. It has efficient in peer to peer message distribution and capable of massive deployment.

3.1 Disadvantages

- Data will be loss
- Overall network performance is low
- Collision occurs during the data transmission in network.

4. Proposed System

In our proposed method use Energy Efficient Location Privacy Preserving Protocol (EELPP) that is an optimization to the Location Aided Routing (LAR). EELPP makes significant reduction in the energy consumption of the mobile nodes batteries through limiting the area of discovering a new route to a smaller zone. Thus, control packets overhead are significantly reduced and the mobile nodes life time is increased. To show the efficiency of the proposed protocol we presented simulations using NS-2. In addition, simulation results show that there is a tradeoff between decreasing control overhead by increasing number of areas and increasing route loss by increasing the number of network areas due to node mobility. This suggests that optimal number of network area is dependent on the nodes mobility. We have to take a different parameters like as throughput, delivery ratio, packet delay on the network.

4.1 Advantages

- Efficiently data will be transmission in the network.
- Improve the network performance.
- Without any data loss on the network.
- It's based in time slot transmission, so data transmission in to easily.
- Very quickly data will reach destination.

4.2 MODULES

4.2.1 Wireless channel design

Wireless relay network to create the one group no of nodes. The packets to send and receiving through the group. It's based transmit scheme of the required for TCP ACK packet drop on the nodes.

4.2.2 Node configuration setting

This module is developed to node creation and more than 10 nodes placed particular distance. Wireless node placed intermediate area. Each node knows its location relative to the sink. The access point has to receive transmitted packets then send acknowledge to transmitter.

4.2.3 Wireless Topology Design

This module is developed to Topology design all node place particular distance. Without using any cables then fully wireless equipment based transmission and received packet data. Node and wireless between calculate sending and receiving packets. The sink is at the center of the circular sensing area.

4.2.4 Multipath routing

Using this module the both source node and destination nodes are to select the multiple path or way in the network. Using the path the nodes are transfer in to without any collision.

4.2.5 Network Address Request

Broadcasts a message requesting an address for a constant number of times after which it assigns itself the first address from the known address block and forms its free node group from the remaining addresses on the networks.

4.2.6 Graph Design Based Result

Graph is an essential part of display a result, so we plot a graph to show a various result comparison with packets, throughput, delay, friends list and etc.

4.2.7 Neighbor set coverage and coverage conditions

We propose a simple distributed approach to determine a small connected dominating set used as the forward node set. Two approaches can be adopted: In the static approach, a connected node set is constructed based on the network topology, but irrelative to any broadcasting. In the dynamic approach, a connected dominating set is constructed for a particular broadcast request, and it is dependent on the location of the source and the progress of the broadcast process. We assume that in the dynamic approach, each node determines its status "on-the-fly" when the broadcast packet arrives at the node. We also assume that the broadcast packet that arrives at v carries information of h most recently visited Nodes for a small h and the corresponding node set is denoted.

4.2.8 Timing issue

A broadcast protocol is called static if the forward/non-forward status of each node is determined on the static view only; otherwise, it is dynamic. The static broadcast protocol is a special case of the dynamic one. The difference is that the forward node set derived from static views can be used in any broadcasting while the one derived from dynamic views is normally used in a specific broadcasting.

4.2.9 Neighbor Discovery Distance model

In this method to using the dimensions are the broadcasting to improving the performance method on the resources of the utilities .The Neighbor Distance Discovery (NDD) method for using to send information quickly and then low latency of network transmission on the process. So we using the most transmission on the network to identify the neighbor node message identify and then sending the data to destination method of the process. It's mostly to use improve the broadcast transmission so we have take the dimension method performance system on the process.

4.2.10 Energy Efficiency

Energy saving techniques at network layer and the routing strategies that allow better energy expenditure and load distribution in order to prolong the network lifetime are considered. After defining a simple energy consumption model to use as reference for the protocol performance evaluation and after introducing some well-known energy based metric, some routing protocols belonging to different families of routing strategies are briefly presented.

5. System Description

5.1 network simulator-2

After setting up the platform, software named ns2 was set up on it which was used for all the analysis and simulation work apart from other tools used. Ns2 is the de facto standard for network simulation. Its behavior is highly trusted within the networking community. It is developed at ISI, California, and is supported by the DARPA and NSF. Ns2 is an object oriented simulator, written in C++, with an OTcl interpreter as a frontend. This means that most of the simulation scripts are created in Tcl. If the components have to be developed for ns2, then both Tcl and C++ have to be used. Ns2 uses two languages because any network simulator, in general, has two different kinds of things it needs to do. On the one hand, a detailed simulation of protocols requires a systems programming language which can efficiently manipulate bytes, packet headers, and implement algorithms that run over large data sets. For these tasks run-time speed is important and turnaround time (run simulation, find bug, fix bug, recompile, rerun) is less important. On the other hand, a large part of network research involves slightly varying parameters or configurations, or quickly exploring a number of scenarios. In these cases, iteration time (change the model and re-run) is more important. Since configuration runs once (at the beginning of the simulation), run-time of this part of the task is less important.

5.1.1 Advantages

- Awirednetwork offerconnection speeds of 100 Mbps to 1000Mbps.
- Physical, fixedwired connections are not prone-to interference andfluctuations in available bandwidth, which can affect some wirelesss networking connections.

5.1.2 Disadvantages

- Expensive to maintain the network due to many cables between computer systems and even if a failure in the cable so it will be very hard to replace that particular cable as it involved more and more costs.
- When using a laptop which is required to be connected to the network, a wired network will limit the logical reason of purchasing a laptop in the first place.

5.2 Wirelessnetworks

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 iteliminates the need for laying out expensive cables and maintenance costs.

5.2.1 Advantages

- Mobile users are provided with access to real-time information even when they are away from their home or office.
- Setting upawireless system is easy and fast and it eliminates the need for pulling out the cables through walls and ceilings.
- Network can be extended toplaces which can not be wired.
- Wireless networks offer more flexibility and adapt easily to changes in th econfiguration of the network.

5.2.2Disadvantages

- Interference due to weather, other radio frequency device, or obstructions like walls.
- Thetotal Through put is affected when multiple connections exists.

5.3 Problems in Wireless Communications

Some of the problems related to wireless communication are multipath propagation, path loss, interference, andlimited frequency spectrum. Multipath Propagationis, when a signal travels from its source to destination, in between there are obstacles which make the signal propagate inpaths beyond the direct line of sight due to reflections, refraction and diffraction and scattering. Pathloss is the attenuation of the transmitted signal strength asitpropagates away fromthe sender. Pathloss can be determined as the ratio between he powers of the transmitted signal to the receiver signal. This is mainly dependent on a number of factors such as radio frequency and then a ture of the terrain. It is sometimes important to estimate thepath loss in wireless communication networks. Due to the radio frequency and the nature of the terrain are not same everywhere, it is hard to estimate the path loss during communication. During communication anumber of signals in the atmosphere interfere with each other resulting in the destruction of the original signal. Limited Frequency Spectrum is where, frequency bands are shared by many wireless technologies and not by one single wireless technology.

5.4 Network Simulator 2.28 (NS2)

Ns-2 is a packet-level simulator and essentially a centric discrete event scheduler to schedule the events such as packet and timer expiration. Centric event scheduler cannot accurately emulate “events handled at the same time” in real world, that is, events are handled one by one. This is not a serious problem in most network simulations, because the events here are often transitory. Beyond the event scheduler, ns-2 implements a variety of network components and protocols. Notably, the wireless extension, derived from CMU Monarch Project, has 2 assumptions simplifying the physical world: Nodes do not move significantly over the length of time they transmit or receive a packet. This assumption holds only for mobile nodes of high-rate and low-speed. Consider a node with the sending rate of 10Kbps and moving speed of 10m/s, during its receiving a packet of 1500B, the node moves 12m. Thus, the surrounding can change significantly and cause reception failure. Node velocity is insignificant compared to the speed of light. In particular, none of the provided propagation models include Doppler effects, although they could.

5.5 Trace Graph

Trace graph is a free tool for analyzing the trace files generated by ns2. Trace graph can support any trace format if converted to its own or ns2 trace format. Trace graph runs under Windows, Linux, and UNIX and MAC OS systems.
Some of the program features are as follows:

- 238 2D graphs: Tracegraph supports drawing 238 different graphs depending upon different parameters in 2 Dimensional areas.
- 12 3D graphs: Tracegraph supports 12 graphs in 3 Dimensions.
- Delays, jitter, processing times, round trip times, throughput graphs and statistics can be plotted with the help of Tracegraph. These are described below:
- Delay: This is the delay encountered between the sending and receiving of the packet.
- Jitter: This is the unwanted variation in the output.
- Processing Time: The time it takes for a node to process the input.
- Round Trip Time: The time required for a signal pulse to travel from a specific source to a specific destination and back again.
- Whole network, link and node graphs and statistics.
- All the results can be saved to text files, graphs can also be saved as jpeg and tiff.
- Any graph saved in text file with 2 or 3 columns can be plotted.
- Script files processing to do the analysis automatically.

The program does have some disadvantages though, such as it hangs or takes a very long time while trying to open large trace files. Also it sometimes hangs after displaying the graph in 3D. The reason why this tool was used in the simulation work is that there are not too many graph plotting tools available in the market.

6. Conclusion and Future work

Extensive arithmetical results have been conduct to support our hypothetically analysis and showthe good quality performances of our solutions. This chapter comprises of complete simulation criteria for considering the resolution of specified objectives and their problem reports simultaneously, that is, the behavior of routing protocols in WMSN by considering the realistic attack traces. The three metrics of PDR E2D THROUGHOUT are evaluated using AODV protocol in three density regions of low density, medium density and high density in network scene as well as in node point.

REFERENCES

[1] VaskenGenc, Sean Murphy, "IEEE 802.16j relay-based Wireless access networks: an overview", October 2008.

[2] Yan Chen, Shunqing Zhang, ShugongXu, and Geoffrey Ye Li, "Fundamental Tradeoffs on Green Wireless Networks", January 25, 2011.

[3] ZiaulHasan, "Green Cellular Networks: A Survey, Some Research Issues and Challenges".

[4] Geoffrey Ye Li, ZhikunXu, "Energy-efficient wireless communications: Tutorial, survey, and open issues", December 2011.

[5] Thomas m. Cover, "Capacity Theorems for the Relay Channel".

[6] DusitNiyato, "Relay-Centric Radio Resource Management and Network Planning in IEEE 802.16j Mobile Multihop Relay Networks" December 2009.

[7] Liam Murphy, "Planning Base Station and Relay Station Locations for IEEE 802.16j Network with Capacity Constraints".

[8] A.S.Syed Navaz, J.Antony Daniel Rex, S.Jensy Mary, "Cluster Based Secure Data Transmission in WSN" International Journal of Scientific & Engineering Research. 6(7), July 2015.

[9] Y. Thomas Hou, "Prolonging Relay Network Lifetime with Energy Provisioning and Relay Node Placement".

[10] Geoffrey Ye Li, ZhikunXu, "Energy-Efficient Wireless Communications: Tutorial, Survey, and Open Issues".

[11] Guo-Hui Lin, "Steiner tree problem with minimum number of Steiner points and bounded edge-length".

[12] DusitNiyato, Ekram Hossain, "Joint Optimization of

[13] Placement and Bandwidth Reservation for Relays in IEEE 802.16j Mobile Multihop Networks".

[14] Nabil H. Mustafa, "PTAS for Geometric Hitting Set Problems via Local Search" June 8–10, 2009.

[15] Congzheng Han, Tim Harrold, "Green Radio: Radio Techniques to Enable Energy-Efficient Wireless Networks".

[16] Hao Feng and Leonard J. Cimini, "On Optimum Relay Deployment in a Multi-Hop Linear Network with Cooperation".

AUTHOR BIBLIOGRPHY

R.KIRUTHIKA, received Bachelor of Computer Application 2011 from Bharathiyar Arts and Science College for Women, Affiliated to Periyar University, Salem, India. She received Master of Computer Application 2014 from *P*ark College of Engineering and Technology, Coimbatore, Affiliated to Anna University-Chennai, India. She is Pursuing M.Phil (full time) from Muthayammal College of Arts & Science, in Periyar University Salem, Tamilnadu, India. Her interested research area is networking.

L.DEVI, Currently doing Ph.D. She received her B.sc Computer Science from Bharathidasan University and MCA from Bharathidasan University. She has completed her M.Phil at Alagappa University. She is having 9 years of experience in collegiate teaching and she is the Associate Professor, Department of PG Computer Science in Muthayammal College of Arts and Science, Rasipuram affiliated by Periyar University. Her main research interests include Network security, Secured multiple path routing in MANET, P2P network IDS.