A Time Slot based Parametric Table Mapping Approach for Wormhole Detection in WSN

Deepika[2]
1Research Scholar, Department of Computer Science and Engineering,
Ganga Institute Of Technology & Management, Kablana

Dr. Yashpal Singh
Assistant Professor
Ganga Institute Of Technology & Management, Kablana

ABSTRACT

Recent advancement in wireless communication and electronics has enabled the development of low cost sensor network. The sensor network can be used for various application areas like military, health, home. Wireless Sensor Network refers to a group of spatially dispersed and dedicated sensors for monitoring and recording the physical conditions of the environment and organizing the collected data at a central location. WSNs measure environmental conditions like temperature, sound, pollution level, humidity, wind speed and direction, pressure etc. WSN is a group of specialized transducers with a communications infrastructure that uses radio to monitor and record the physical condition. WSN provide a bridge between the real physical and virtual world. It allows the ability to observe the previously unobservable at a fine resolution over large spatio-temporal scales.

A sensor network consists of multiple detection stations called sensor nodes, each of which is small, lightweight, portable. Every sensor node is equipped with a transducer, microcomputer, transceiver and power source. A wireless sensor network is a group of specialized transducers with a communications infrastructure for monitoring and recording conditions at diverse locations. Commonly monitored parameters are temperature, humidity, pressure, wind direction and speed, illumination intensity, vibration intensity, sound intensity, power-line voltage, chemical concentrations, pollutant levels and vital body functions. A sensor network consists of multiple detection stations called sensor nodes, each of which is small, lightweight and portable.

The WSN is an emerging technology in the field of communication. This technology has many advantages but the security issues have been not given much consideration till now.

▪ INTRODUCTION

Wireless Sensor Networks can be considered a particular type of Mobile Ad-hoc Network, formed by hundreds or thousands of sensing devices communicating by means of wireless transmission. Research on WSNs and MANETs share similar technical problems. Wireless Sensor Networks are formed by a large number of networked sensing nodes. It is rather complex, or even unfeasible, to model analytically a WSN and it usually leads to oversimplified analysis with limited confidence. Besides, deploying test-beds supposes a huge effort.

Nodes: Each node is a physical device monitoring a set of physical variables. Nodes communicate with each other via a common radio channel. Internally, a protocol stack controls communications. Unlike classical network models, sensor modes include a second group of components: The physical node tier, which is connected to the environment. Nodes are usually positioned in a two or three dimensional

ISSN: 2278 – 1323

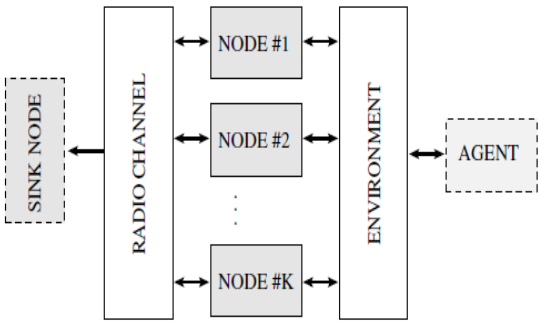
world. An additional "topology" component, not showed in figure may control node coordinates. Depending on the application and deployment scenario, a WSN can contain from a few to several thousands of nodes.

Environment: The main difference between classical and WSN models is the additional "environment" component. This component models the generation and propagation of events that are sensed by the nodes, and trigger sensor actions, i.e. communication among nodes in the network. The events of interest are generally a physical magnitude as sound or seismic waves or temperature.

Radio channel: It characterizes the propagation of radio signals among the nodes in the network. Very detailed models use a "terrain" component, connected to the environment and radio channel components. The terrain component is taken into consideration to compute the propagation as part of the radio channel, and also influences the physical magnitude.

Sink nodes: These are special nodes that, if present, receive data from the net, and process it. They may interrogate sensors about an event of interest. The use of sinks depends on the application and the tests performed by the simulator.

Agents: A generator of events of interest for the nodes. The agent may cause a variation in a physical magnitude, which propagates through the environment and stimulates the sensor. This component is useful when its behavior can be implemented independently from the environment, e.g., a mobile vehicle. Otherwise, the environment itself can generate events.



- **WHAT MAY WEXPECT FROM A GOOD WSN SIMULATOR?**

Usually, the key properties to select suitable simulation environment are:
1) Reusability and availability.
2) Performance and scalability.
3) Support for rich-semantics scripting languages to define experiments and process results.
4) Graphical, debug and trace support.

Reusability and availability: Simulation is used to test novel techniques in realistic and controlled scenarios. Researchers are usually interested in comparing the performance of a new technique against existing proposals. Therefore, two key aspects are: Does the simulation tool include implementations of common models? How easy is to modify or integrate a new model with the existing ones? The first question mainly depends on how long a framework has been used for, and how many people use it. Early and widely adopted frameworks have many available models and it is very likely that the new successful proposals will be added to next releases. The second aspect is closely related to the design of the package. A careful structure with clean interfaces and high modularity allows the user to easily add or change functionality. Ready-to-use models allow users to quickly build a realistic simulation scenario and focus on modeling more specific details of WSN.

Performance and scalability: Performance and scalability is a major concern when facing WSN simulation. The former is usually bounded to the programming language effectiveness. The latter is constrained to the memory, processor and logs storage size requirements. Additionally, the type of simulation implies some limits: Emulation mode and time-driven simulations operate in real time so they cannot be arbitrarily long. Wireless simulations stress performance and scalability issues due to the increased complexity added by the interaction with the environment, radio propagation, mobility and power consumption. Simulation of several hundred of thousands of nodes remains a challenging problem.

Support for rich-semantics scripting languages to define experiments and process results: The configuration of a WSN typical trial requires to answer questions like: How many nodes are there in the test?, where is each node placed?, do nodes move?, all of them?, how?, which energy model is used?, how many physical environments are?, how they generate events?, which physical magnitudes should measure each node?, which statistics must be measured in the experiment?,

ISSN: 2278 – 1323

which are the parameters of the radio model? The vast amount of variables involved in the definition of a WSN experiment requires the use of specific input scripting languages, with high-level semantics. Additionally, it is likely that large quantities of output data will also be generated through many replicas of the experiments. Therefore, a suitable output scripting language, that helps to obtain the results from the experiments quickly and precisely is desirable.

Graphical, debug and trace support: Graphical support for simulations is interesting in three aspects:
(1)As a debugging aid. The primary and more practical way to quickly detect a bad behavior is to "watch" and follow the execution of a simulation. The key features that a graphical interface should support are: Capability of inspection of modules, variables and event queues at real time, together with "step-by-step" and "run-until" execution possibilities. These features make graphical interfaces a very powerful debugging tools. Note that the key is the ability to interact with the simulation.
(2) As a visual modeling and composition tool. This feature usually facilitates and speeds the design of small experiments or the composition of basic modules. However, for large scale simulations, it is not very practical.
(3) Finally, as result plotters, which allows quick visualization of results without a post-processing application.

▪ SECURITY

Wireless sensor nodes network means that shares common property as computer network. So we need security issues: - **Attack and Attacker***:* - Attack means that unauthorized person access to a service. For security we need secure resource or information we need integrity, availability, or confidentiality of a system. Attackers can create fault and weakness in a security design, implementation, configuration or limitation are occurs.

Authentication: WSNs transfer information and sensitive data for different important decision making. Receiver wants to the data with ensure that are correct source for decision-making process [10]. Authentication provides proof to sender node and receiver that data is secure in which they want to communicate.

Integrity: Integrity means ensure that there must no tampering and extra data. Receiver check that data received is exactly original and same as send by the sender. Data integrity is to ensure that information is same during transmission by using some security key for ensure.

Confidentiality: It gives guarantee that data send by the sender will not access by attacker. Encryption key is used for sending the message. Confidentiality means create security from unauthorized parties and attacker.

Scalability: Scalability means that no node compromise and no increase communication when size of network is grow. It should allow nodes to be added in network with proper deployment as well.

Self-Organization: In WSN Every sensor node is in dependent and flexible enough to be self organizing in different environments. No fixed infrastructure is available for WSN Network management. In self organizing we used conduct key management. In self organization we used conduct key management and building trust relation among sensor for security.

▪ ATTACKS IN WSN

In wireless sensor network nodes are present on hostile or dangerous environment at that environment they are not physical protected. Attack and Attackers are means that unauthorized process that disturb the security service. A various types of attacks are possible in Wireless Sensor Network (WSN). Security attacks in WSN and all other networks can be roughly classified by the following criteria: Based on the Capability of the attacker, Attack on

ISSN: 2278 – 1323

information in transit, Host based Vs Network based, Based on protocol layer, Attack on communication, Stealthy or Non-Stealthy.

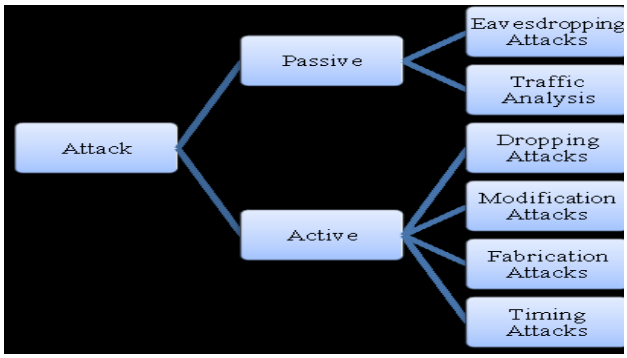
Passive attacks: Process of monitoring and listing of the communication channel is done by unauthorized attackers. Data exchanged without interruption the communication

.

Active attacks: Unauthorized attacker can make some change on the data stream of the communication channel are known active attack. It disturb the normal function of the network, meaning information interruption, modification or fabrication.

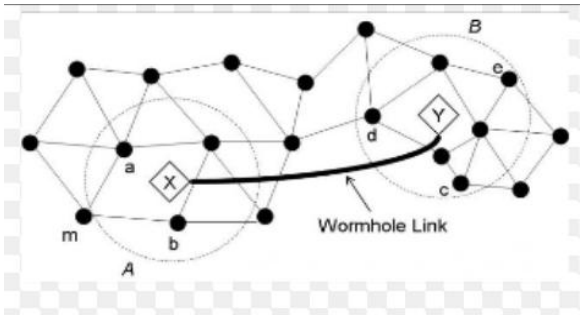
Host Based Vs Network Based

During compromising users of WSN:- By cheating user share information like as password or keys about the sensor nodes. Two types compromise hardware and software. In hardware involve tempering with the hardware to extract the programming code and data and keep store with in sensor node. In software compromise involve breaking the software running on sensor node. Network attacks compromise old on layer specific and protocol specific. In this, attacker's purpose not disturbs the service availability, message confidentiality and security but gain an unfair advantage for itself in the usage of network.



▪ WORMHOLE ATTACK

Wormhole is a type of link in which two attacker nodes creates a link call wormhole link by which both the nodes can communicate. These nodes give an illusion that the selected path is the shortest path to get the destination. Here the attackers build an overlay tunnel over the existing wireless medium. This attack is potentially very much harmful and is the most preferred choice of attackers.



Wormhole attack like as a denial of service attack that disturb the network communication infrastructure without knowledge of the cryptography key methods. In wormhole attack may be created by a single or a pair of collaborating nodes in which two or more attackers are connecting by high speed off-channel link called wormhole link. A wormhole attack could be launched in two different modes: hidden and participation mode. In wormhole attack modes are depending upon attackers add their identity into packet headers when tunneling and replaying messages. In hidden mode attackers are not seen by the legitimate nodes. In this mode attackers put him on powerful position and during transmission capture message at one end of the wormhole and replicate them at the another end. This mode not need information about the authentication and encryption because its purpose only disturb and confused routing mechanisms. In this way it can create a virtual link

ISSN: 2278 – 1323

between two far-off nodes by for example "tunneling" the hello messages. So that hidden-mode wormhole attack is more difficult to defend against it. In participation mode attackers acquire valid cryptographic keys to attack on legitimate nodes. In this mode an attacker no need to create virtual link between the legitimate nodes. But they participate in the routing as legitimate node and use the wormhole to modify the original packet. This mode also very difficult to detect since the malicious nodes can simply ignore the security mechanisms of routing protocol.

Wormhole Attack Model:-Wormhole attack is a network layer attack (like as DoS) that can affect the network communication infrastructure without the knowledge of cryptographic techniques implemented. This is the reason why it is very difficult to detect. It is bombard by one, two or more number of nodes. In wormhole link it can create two ended wormhole, one end tunnels the packets and other end on receiving packets, replays them to local area. According to modes wormhole attack is classified into three models of wormhole attack like as closed, half open and open.

- **TYPES OF WORMHOLE ATTACK**

Number of nodes involved in establishing wormhole and the way to establish it classifies wormhole into following types.

Wormhole using Packet Encapsulation:- In encapsulation-based wormhole attack, several nodes exist between two malicious nodes and data packets are encapsulated between the malicious nodes. Only encapsulated packet message transfer no hop count incrementing. Here several nodes exist between two malicious nodes and data packets are encapsulated between the malicious nodes. Hence it prevents nodes on way from incrementing hop counts. The packet is converted into original form by the second end point. This mode of wormhole attack is not difficult to launch since the two ends of wormhole do not need to have any cryptographic information, or special requirement such as high-power source or high bandwidth channel.

Wormhole using Out-of-Band Channel:- In this attacker create out-of-band with high bandwidth channel in between two-end points in wormhole link. This kind of wormhole link only used one malicious node with high transmission capability in the network that attracts transmission of the intermediates node path that is passing from it. This mode of attack is more difficult to launch than the packet encapsulation method since it needs specialized hardware capability. Consider the outline presented in fig.. In wireless sensor network W_1 and W_2 are malicious nodes and they have an out-of-bound channel between themselves. Let us assume that source node (S) sends a RREQ to sink node and nodes A and W_1 are neighbors of S. Node W_1 transfer the RREQ to W_2 and W_2 broadcasts the message to its neighbors, including the sink node.

Sink node receives two RREQs: (S-W_1-W_2-Sink) and (S-A-B-C-Sink), sink node choose the first route because first route is faster and shorter than second than first route create out-of-bound modes of attack.

Wormhole using Packet Relay:-One or more malicious nodes can launch packet-relay-based wormhole attacks. In this type of attack malicious node replays data packets between two far nodes and

ISSN: 2278 – 1323

this way fake neighbours are created. This kind of attack is also called as "replay-based attack".

Wormhole using Protocol Distortion:-In this mode of wormhole attack, single malicious node tries to attract network traffic by distorting the routing protocol. This mode does not affect the network routing much and hence is harmless. Also it is known as "rushing attack".

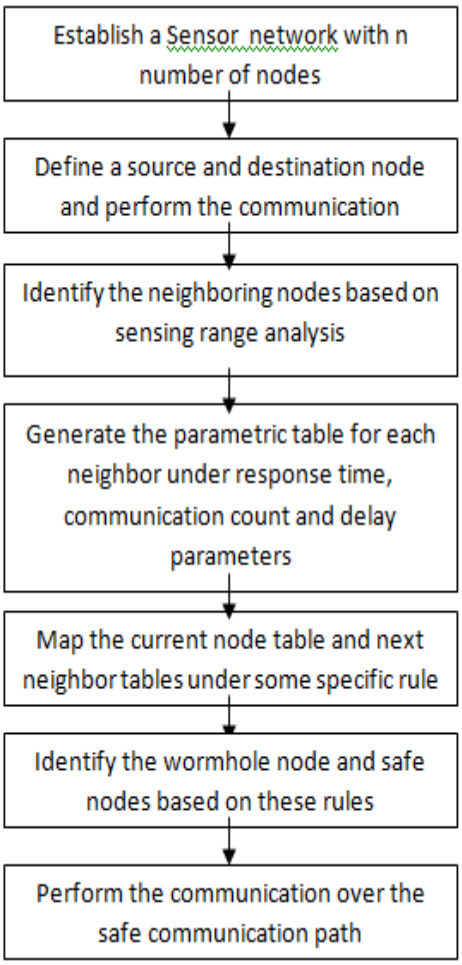
▪ PROBLEM STATEMENT

A sensor network is a dynamic reconfigurable network with heavy traffic over the network. As the network is available widely, there are more chances of inclusion of external nodes that behave as the attack node. One of the problems in sensor network is the wormhole attack. In two nodes creates a communication tunnel and does provide communication with other nodes. If some communication goes to these nodes, they start communicating in the same tunnel so that whole communication disturb and degrades. In this work, a periodic table driven crosscheck approach is defined to analyze the trust level of neighbor nodes. In this work, as the communication path will be defined, an analysis to the neighboring node will be performed by current communicating hop. This hop will generate the neighbor list table under trust vector. This trust vector will store the number of neighboring nodes along with its response time, delay and connective communication analysis. Once table will be generated, the mapping between the current hop table and next feasible hop table will be done under these estimated parameters. The neighbor with minimum connectivity will be considered as wormhole node. Here the rules will be defined for identification of wormhole nodes as well as best neighbor node. This identified best neighbor will be set as next effective hop. This process will be repeated till the communication path between source and destination is not build. The work will be implemented in omnet++, The analysis of work will be done in terms of throughput and communication delay parameters.

▪ RESEARCH METHODOLOGY

A sensor network is one of the critical adhoc network in which nodes communicated cooperatively to deliver the information. But because of this cooperative nature, the network suffers from various kind of attacks. One of such critical attack is worm hole attack. The presented work is defined to provide the solution against wormhole attack. In this work, a time slot based table mapping approach is defined. The work will be able to identify the wormhole attack over the network as well as indentify the safe communication path between the source and destination node. The flow of presented work is given here under

ISSN: 2278 – 1323



- **ALGORITHM**

WormHoleDetection(Nodes)

/*Nodes is the list of sensor nodes with specification of worm hole in the network to identify the attack situation and to identify the worm hole attack in the network*/

{

1. Set Source node Src and Destination Node Dst for the network

2. Set CurNode=Src

   [Set source as current Node

3. While (CurNode<>Dst)

   [Repeat the Process till destination node not occur]

   {

2. For i=1 to Nodes.length

   [Process All Nodes]

   {

3. if(GetRespoonse(Src,Nodes(i))<SensingThreshold)

   [Check for valid neighbor node]

   {

4. Throughput=GetCommunication(Nodes(i))

   [Get the communication relative to the Current Node]

5. if(Loss(Nodes(i))>Threhsold)

   [If the Loss Occur for the communication Node]

   {

6. if(Frequency(Nodes(i)>FThreshold And Throughput<TThresholod

   [If communication over the node is higher then normal)

   {

7. Set Nodes(i).Type=”WormHole”

   [Set the Node type to WormHole if the communication is abnormal and having the loss over the node]

   }

   }

   }

   }

8. Else

ISSN: 2278 – 1323

{

9. Set CurNode=EffectiveNode(Nodes)

[Identify high throughput node as next hop]

}

}

▪ TOOL USED

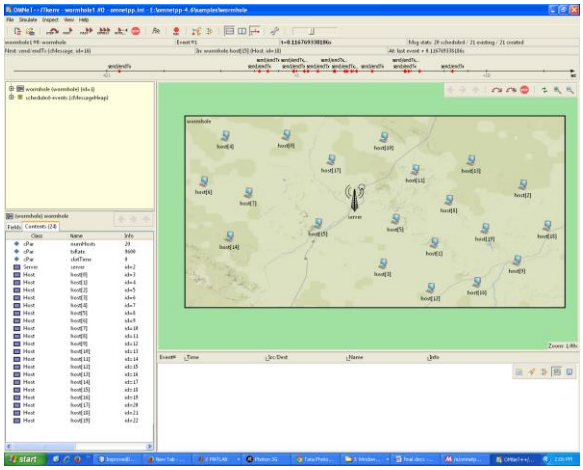
OMNeT++ stands for Objective Modular Network Testbed in C++. It is a discrete event simulation tool designed to simulate computer networks, multi-processors and other distributed systems. Its applications can be extended for modelling other systems as well. It has become a popular network simulation tool in the scientific community as well as in industry over the years. The principal author is András Varga, with occasional contributions from a number of people.

❖ COMPONENTS OF OMNET++:

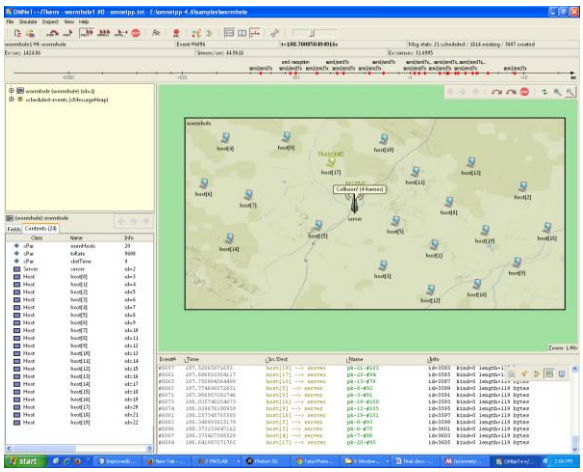
- ✓ simulation kernel library
- ✓ compiler for the NED topology description language (nedc)
- ✓ graphical network editor for NED files (GNED)
- ✓ GUI for simulation execution, links into simulation executable (Tkenv)
- ✓ command-line user interface for simulation execution (Cmdenv)
- ✓ graphical output vector plotting tool (Plove)
- ✓ utilities (random number seed generation tool, makefile creation tool, etc.)
- ✓ documentation, sample simulations, contributed material, etc.

▪ RESULT

➢ Simulation Network

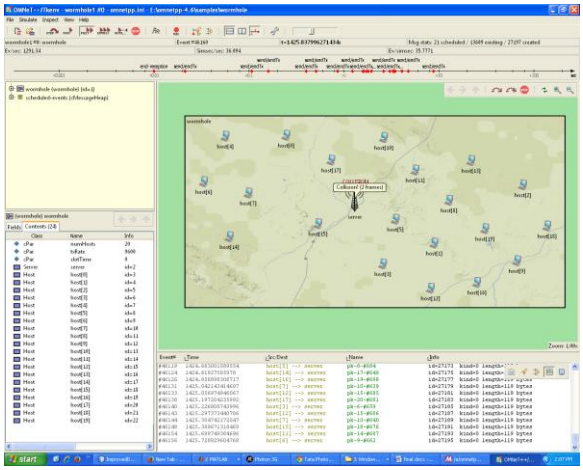


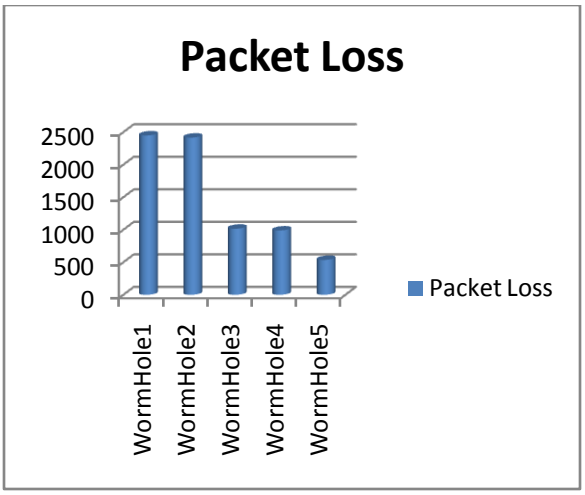
➢ Successful Communication



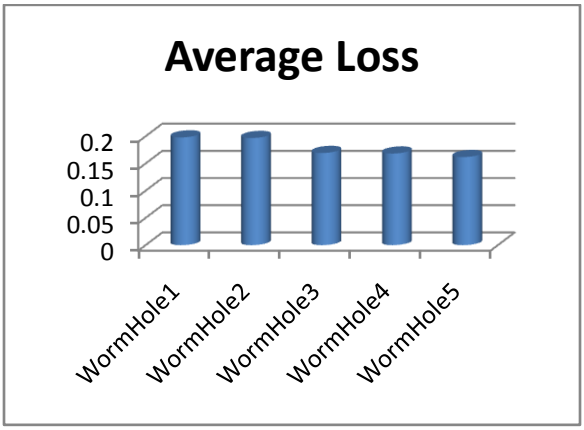
➢ Attacked Communication

ISSN: 2278 – 1323

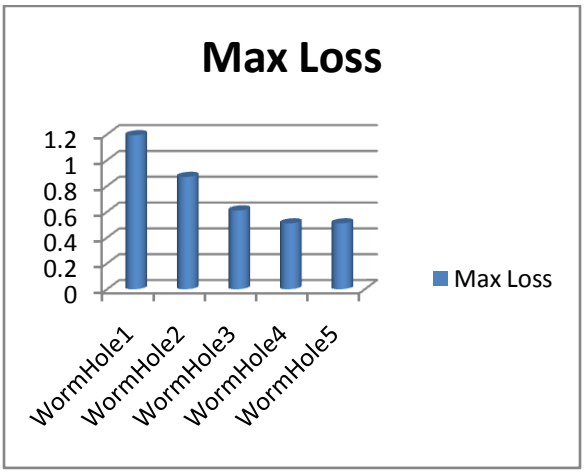




➢ Average Loss Analysis



➢ Maximum Loss Analysis



➢ Packet Loss Analysis

▪ CONCLUSION

The presented work is defined to provide the safe communication in worm hole infected network. The work is defined on critical sensor network to provide the safe communication over the network. The work is provided as an improvement to the dynamic routing approach in which at first the worm hole node is identified and later on the communication is performed over the safe nodes. The communication analysis is here done under throughput, response time, loss and node frequency analysis. The work is here implemented in OMNet++ environment. The results shows that the work has reduced the communication loss and communication delay and improved the communication throughput.

▪ REFERENCES

[1]. M.Parsons and P.Ebinger, "Performance Evaluation of the Impact of Attacks on mobile Ad-Hoc networks"IEEE, vol.40, no.10, pp. 70- 75, October 2010.

[2]. D.B.Roy, R.Chaki and N.Chaki, "A New Cluster-Based Wormhole Intrusion etection Algorithm for Mobile Ad-Hoc Neworks,"

ISSN: 2278 – 1323

International Journal of Network Security and Its Application (IJNSA), Vol. 1, No.1, April, 2009.

[3]. N.Shanti, Lganesan and K.Ramar, "Study of Different Attacks On Multicast Mobile Ad-Hoc Network".

[4]. C.Wei, L.Xiang, B.yuebin and G.Xiaopeng, "A New Solution for Resisting Gray Hole Attack in Mobile Ad-Hoc Networks," Second International Conference on Communications and Networking in china, pp.366-370, Aug, 2007.

[5]. S.Marti, T.J.Giuli, K.Lai, M.Baker, "Mitigating Routing Misbehavior in Mobile Ad-Hoc Networks".

[6]. F.Stanjano, R.Anderson, "The Resurrecting Duckling: Security Issues for Ubiquitous Computing," Vol. 35, pp. 22-26, Apr, 2002.

[7]. K. Biswas and Md. Liaqat Ali, "Security threats in Mobile Ad-Hoc Network", master Thesis, Blekinge Institute of Technology" Sweden, 22nd March 2007

[8]. G. A. Pegueno and J. R. Rivera, "Extension to MAC 802.11 for performance Improvement in MANET", Karlstads University, Sweden, December 2006

[9]. Deng H., Li W. andAgrawal, D.P., "Routing security in wireless ad hoc networks," ommunications Magazine, IEEE, vol.40, no.10, pp. 70- 75, October 2002.

[10]. Al-Shurman, M., Yoo, S. and Park, S, "Black hole Attack in Mobile Ad Hoc Networks", ACM Southeast Regional Conference, pp. 96-97, 2004.

[11]. Tamilselvan, L.; Sankaranarayanan, V., "Prevention of Blackhole Attack in MANET," ireless Broadband and Ultra Wideband Communications, 2007. Aus Wireless 2007. The 2nd International Conference on, vol., no., pp.21, 27-30 Aug. 2007.

[12]. Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, YoshiakiNemoto, Detecting Black hole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method" International Journal of Network Security, Vo l.5, No .3, P P.338–346, Nov. 2007.

[13]. LathaTamilselvan, V. Sankaranarayanan, "Prevention of Co-operative Black Hole Attack in MANET", Journal of Networks, Vol 3, No 5, 13-20, May 2008[6] Zhao Min; Zhou Jiliu, "Cooperative Black Hole Attack Prevention for Mobile Ad Hoc Networks", Information Engineering and Electronic Commerce, 2009. IEEC '09.International Symposium on, vol., no., pp.26-30, 16-17 May 2009.

[14]. Ming-Yang Su; Kun-Lin Chiang; Wei-Cheng Liao, "Mitigation of Black-Hole Nodes in obile Ad Hoc Networks," Parallel and Distributed Processing with Applications (ISPA), 2010 International Symposium on, vol., no., pp.162-167, 6-9 Sept. 2010.

[15]. Alem, Y.F.; Zhao Cheng Xuan; , "Preventing black hole attack in mobile ad-hoc networks using Anomaly Detection," Future Computer and Communication (ICFCC), 2010 2nd International Conference on , vol.3, no., pp.V3-672-V3-676, 21-24 May 2010.

[16]. Medadian, M.; Mebadi, A.; Shahri, E., "Combat with Black Hole attack in AODV

ISSN: 2278 – 1323

routing protocol", Communications (MICC), 2009 IEEE 9th Malaysia International Conference on, vol., no., pp.530-535, 15-17, Dec.2009.

[17]. XiaoYang Zhang; Sekiya, Y.; Wakahara, Y., "Proposal of a method to detect black hole attack in MANET," Autonomous Decentralized Systems, 2009. ISADS '09. International Symposium on, vol., no., pp.1-6, 23-25 March 2009

[18]. Songbai Lu; Longxuan Li; Kwok-Yan Lam; LingyanJia, "SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack," Computational Intelligence and Security, 2009. CIS '09. International Conference on, vol.2, no., pp.421-425, 11-14 Dec. 2009.

[19]. NitalMistry, Devesh C Jinwala, MukeshZaveri, "Improving AODV Protocol against lackhole Attacks", proceedings of the International Multi Conference of Engineers and Computer Scientists 2010 Vol II, IMECS 2010.

[20]. Yaserkhamayseh, Abdulraheem Bader, Wail Mardini, and MuneerBaniYasein, "A New Protocol for Detecting Black Hole Nodes in Ad Hoc Networks", International Journal of Communication Networks and Information Security (IJCNIS) Vol. 3, No. 1, April 2011.

[21]. Payal N. Raj1 and Prashant B. Swadas2, "DPRAODV: A Dynamic Learning System against Blackhole Attack in AODV based MANET", IJCSI International Journal of Computer Science Issues, Vol. 2, 2009.

[22]. Mohammad Abu Obaida, Shahnewaz Ahmed Faisal, Md. Abu Horaira, Tanay Kumar Roy, "AODV Robust (AODVR): An Analytic Approach to Shield Ad-hoc Networks from Black Holes" International Journal of Advanced Computer Sciences and Applications, Vol: 2 Issue: 8 Pages: 97-102, 2011.

[23]. Subash ChandraMandhata, Dr.Surya Narayan Patro, "A counter measure to Black hole attack on AODV- based Mobile Ad-Hoc Networks" International Journal of Computer & Communication Technology (IJCCT), Volume-2, Issue-VI, 2011.

[24]. LalitHimral, Vishal Vig, Nagesh Chand, "Preventing AODV Routing Protocol from lack Hole Attack" International Journal of Engineering Science and Technology (IJEST) Vol. 3 No. 5, May 2011.

[25]. K. Lakshmi1, S.Manju Priya2 A.Jeevarathinam3 K.Rama4, K. Thilagam5, "Modified AODV Protocol against Blackhole Attacks in MANET", International Journal of Engineering and Technology Vol.2 (6), 2010.

[26]. Herminder Singh, Shweta "An approach for detection and removal of Black hole In ANETS" International Journal of Researh in IT& Management (IJRIM) Volume 1, Issue 2 (June, 2011).

[27]. KamarularifinAbd. Jalil, Zaid Ahmad, Jamalul-LailAbManan, "Mitigation of Black hole Attacks for AODV Routing Protocol", Society of Digital Information and Wireless Communications (SDIWC) Vol01_No02_30, 2011.

[28]. Sen, J.; Koilakonda, S.; Ukil, A.; , "A Mechanism for Detection of Cooperative Black Hole Attack in Mobile Ad Hoc

ISSN: 2278 – 1323

Networks", Intelligent Systems, Modelling andSimulation (ISMS), 2011 Second International Conference on , vol., no., pp.338-343, 25-27 Jan. 2011.

[29]. Osathanunkul, K.; Ning Zhang; , "A countermeasure toblack hole attacks in mobile ad hoc networks," NetworkingSensing and Control (ICNSC), 2011 IEEE InternationalConference on, vol., no., pp.508-513, 11-13 April 2011.

[30]. N. Bhalaji, A. Shanmugam, "A Trust Based Model to Mitigate Black Hole Attacks n DSR Based MANET", European Journal of Scientific Research, Vol.50 No.1, pp.6-15, 2011.

[31]. C.Perkins, "(RFC) Request for Comments – 3561", Category: Experimental, Network, Working Group, July

ISSN: 2278 – 1323