International Journal of Current Trends in Engineering & Technology
www.ijctet.org, ISSN: 2395-3152
Volume: 04, Issue: 01 (January- February, 2018)

A Novel Security Scheme against Wormhole Attack in WSN

Poonam Pawar[1], Kamlesh Chandravanshi[2]
Department of Computer Science & Engineering
Technocrats Institute of Technology, Bhopal
[1]poonampawar127@gmail.com, [2]kamlesh.vjti@gmail.com

Abstract—*Wireless Sensor Network (WSN) is comprised of hosts capable of functioning in absence of infrastructure. Such networks should be capable of self forming, self organizing, self managing, self recovering, and able to operate under dynamic conditions. The multi-hop communication phenomenon is used to sending information to receiver. To attain this, each mobile node depends on its neighbor or range node to forward the data packet to the destination. In fact, most of previous studies on WSNs have implicitly assumed that nodes are cooperative As such; the node cooperation becomes a very important issue in WSNs. The attacker in WSN are easily affected the routing performance by that the data receiving ratio is affected as comparable to normal routing performance of in dynamic network and dropping of data is enhanced. In this research we proposed new neighbor identification based IDS (Intrusion Detection System) of detecting routing misbehavior through wormhole attack. The wormhole attacker nodes uniqueness is to making the tunnel and replies the positive acknowledgement of destination at time of flooding routing packets and drops the data packets deliver through tunnel created by attacker. The attacker is identified by the past and current data receiving and forwarding in dynamic network. The attacker is block through the broadcasting scheme used by IDS from their actual identification to neighbors. The IDS nodes are block the communication of attacker and provide the secure communication among the mobile nodes in WSN. The performance of proposed security against wormhole attack is measure through performance metrics like PDF and attacker Infection.*

Keywords:-WSN, Routing, Malicious, worm hole, IDS.

I. INTRODUCTION

The wireless in dependent network that forming topology itself and nodes are behaves like sender, receiver and router. All the nodes in Wireless sensor Network (WSN) operating in limited area with none control of centralized administration [1]. In WSN all the nodes are operating in an open surroundings with none interference of any authority that's why security is usually also affected. The detector networks are of 2 types:-

A. Decentralized WSN

In this style of network the full mobile sensors are communicate with one another and exchange their info in dynamic environment. The proposed work is done in field of security is decentralized WSN against wormhole attack.

B. WSN with Base station or Servers.

The base station in detector network is collecting data from totally different sources and each sensor node is forward this information to different node until the base station isn't found. It may be possible the nodes are mobile and stationary. The base station is forward similar collected information into web if needed. The nodes in WSN could leave or be part of the network at any purpose of your time, thereby considerably moving the standing of trust among nodes and also the complexness of routing. Such quality entails that the topology of the network moreover because the property between the hosts is unpredictable. That the management of the network environment may be a function of the participating nodes. Owing to this absence of centralized authority, straight techniques of network supervising and security don't seem to be quite obligatory for WSN. Many attacker or malicious node within the network can agitate the full procedure or can even stop it. Associate example of a detector Network is given in figure one.1 wherever nodes are act directly with one another. All the links between nodes are wireless. The network is following the shortest path routing technique for sending information in between sender and receiver.

Bluetooth [1, 2] may be a typical example of such networks however that has solely in terms of sense of neighbor and information transferring. The multi-hop communication is feasible however not economical in Bluetooth, The routing of knowledge is thru totally different hops to destination is simply potential in dynamic network. The networks are freelance of any mounted infrastructure or central entity like cellular networks [2, 3] which needs mounted infrastructure to control. In order to take care of the supply of a WSN, resilience to node failure is extremely vital. One of the ways in which a WSN node may fail is thru associate attack. Several WSN routing protocols are designed but none are designed with security as a main goal. WSNs are at risk of a spread of security attacks owing to the published nature of the transmission medium and also the proven fact that detector nodes typically operate in hostile environments.

This paper is organized as follows: Section 2 is the overview of routing protocols and Section 3 covers the related work. Section 4 is proposed scheme is defined in detail and Section 5 is the description of simulation environment. Section 6 is the explanation of simulation results in details and Conclusion and future work is given in Section 7.

II. OVERVIEW OF ROUTING PROTOCOLS

A Sensor Network consists of many nodes. Knowledge packets on transit normally tolerate many nodes before eventually reaching the destination. Routing is that the act of crucial the trail to be followed by a packet so as to achieve its desired destination. To do this, variety of things got to be taken into consideration. Routing protocols takes charge of this method. Quite a variety of protocols [5, 6], e.g. DSDV, AODV, DSR and TORA are planned for ancient ad hoc wireless networks. However, they're not suited to the distinctive options and application needs of WSNs. the planning of routing protocols for WSNs may be a difficult task that has been within the focus of the device network analysis community within the recent past [4]. WSN routing protocols has been planned. The planned protocols

show a high selection that stems from the various needs of the varied unreal application situations. First of all, links in WSNs are usually unreliable and not stable as a consequence of the low transmission power, the chip antenna style, and also the indisputable fact that the nodes are usually placed arbitrarily distributed on the base.
Moreover, link breaks is also caused by e.g. asynchronous sleep times, interference, moving obstacles, energy exhaustion, node failure or quality. Thus, the topology of the network changes often that represents a difficult downside for the routing protocol style since the device nodes also are terribly restricted in their process power and memory.

A. Classification of Routing Protocols

Broadly speaking, most of the routing protocols may be classified consistent with the network structure; as flat, gradable or location-based. Further, these protocols may also be classified consistent with operation mode; multipath-based, query-based, negotiation-based, QoS-based, and coherent-based [5]. Routing protocols that are designed for mesh and ad hoc networks are sometimes classified consistent with the method they establish routes within the network [6]. This type of classification is additionally terribly practicable for WSN routing protocols. There exist 3 totally different classes. The primary one is named proactive. Proactive protocols try and establish and maintain routes before they're required. The second class is portrayed by reactive protocols that follow the contrary approach wherever routes are solely established or computed on demand. The last cluster consists of hybrid protocols that mix the ideas of reactive and proactive route institution.

III. RELATED WORK

In the section of related we mentioned the work that has done in the field of wormhole attacker to prevent and detect and also affect of attack in routing protocols.

Raja Waseem Anwar, Majid Bakhtiari, Anazida Zainal,Abdul Hanan Abdullah and Kashif Naseer Qureshiwe in this paper [7] proposed an enhance version of AODV hello packets. The study assumes some assumption to use our propose methodology like the clock time is synchronized and used throughout neighbor discovery. Neighbor nodes respond with appending hullo massage with gift received time and reply. The approximate distance between two node time is calculated If distance is greater than sender node most transmission capability then wormhole is suspected and ignore suspicious neighbor and choose discover an alternate route. If it fails in this method then propose approach implement and trust-reply packet send to verify the packet delivery to destination. Research Drawbacks: - The range of attackers is considered in delay graph is forty five however wormhole attacker is two nodes then the entire range of nodes is needed ninety however in this analysis total range of nodes is eighty considered. The terrain size is tiny by that nodes are moves in a restricted space. Property simply obtainable. The loss performance of offender isn't mentioned.

Soo-Young Shin, Eddy Hartono Halim in this paper [8] proposed approach consists of three parts that are routes redundancy, routes aggregation and round-trip-time calculation. Researchers have a tendency to use 1st phase to form a multipath transmission to confirm that the RREQ is absolutely sent to the destination. Second phase is employed to mixture similar methods together with their addresses, therefore destination and supply apprehend each potential valid route which will be used. Last phase is employed to calculate the average range of hops in keeping with its round-trip time and investigates the probability of wormhole attackers by comparing range of hops and its average time of each route from the list received by supply. All malicious nodes that thought of as attackers is isolated and born from network. The RTT and range of hops of all listed routes are compared so as to notice suspicious route. Nodes with suspicious behavior among network are isolated and cannot be thought-about for transmission. The drawbacks of this analysis and benefits of my analysis are: - Multipath transmission is employed to check the responsibility of path however we have a tendency to test the responsibility in unipath routing. The procedure of RTT is a lot of advanced as a result of to examine the RTT price in every link however we have a tendency to don't seem to be reckoning on the RTT price. Only packet dropping performance is measured here, remainder of the performance metrics isn't measured here but we evaluate the performance of all performance metrics. Infection proportion means that how much proportion of information is affected from attack don't seem to be value in each the previous researches, however we measure it.

Ravinder Ahuja, Alisha Banga Ahuja, Pawan Ahuja in this paper [9] evaluated the performance of on demand routing protocols unintended on demand distance vector routing (AODV) and dynamic supply routing (DSR) with and while not wormhole attack. They've taken three performance parameters i.e. packet delivery ratio, throughput, and average finish to finish delay. The results are showing that performance of routing protocol decreases beneath the wormhole attack. Therefore a decent solution got to be ascertaining which may offer strength to routing protocols to notice and defend against wormhole attack. Next we are going to offer solution that may notice and defend the wormhole attack so network and routing protocols functioning isn't disturbed. In this paper only the impact of attack is observe in numerous routing protocols however no security theme is proposed to secure network from wormhole attack.

Towards intrusion detection in [10] introduce a light-weight theme for detecting selective forwarding and part attacks in WSN. The key plan of their theme is to form nodes monitor their neighborhood then communicate between one another to make a decision if there's an intrusion taken place. The scheme is any evaluated by experimentation on a true WSN readying. This theme edges from the neighbors observance so there's a form of distribution that may minimize the computation load on a detection agent node. However, can be a rise within the communication messages between nodes throughout the collaboration for selection that may increase the communication overhead and as a result will consume the ability of nodes quickly. It's clear that, this theme lacks the generality that different schemes within the same class.

Intrusion notice on theme of depression attack in WSN is a lot of specific intrusion detection theme to detect depression attack was proposed by [11]. This theme consists of 4 modules: local Packet observance Module, native Detection Engine Module, Cooperative Detection Engine and native Response Model. The proposed theme has been enforced within the TinyOS surroundings with Min Route protocol. An acceptable detection rules are ready to suite with the depression attack. Generally, this theme satisfies the distribution feature of IDS that is extremely needed on a large scale and autonomous surroundings like WSN. The matter here still with the communication overhead between the nodes to exchange helpful data that helps in detecting the attack.

P. Vittorio, Illiano and C. Emil, Lupu [12] in this paper, thought of directly the scenario wherever an offender gains full control of one or a lot of sensors and may run arbitrary malware on them to fabricate new measurements and report them in situ of the ascertained ones. Their task consists of sleuthing the incongruities between the ascertained and the according measurements. Although, in surroundings manipulation situation there's no incongruousness between ascertained and according measurements, an according measuring still differs from what would be according within the absence of attacks. In each case the non compromised measuring is an unknown variable, therefore it has to be characterized through evident properties, which successively don't seem to be compromised. The approach pursued during this analysis relies on measurements analysis and its applicability depends on the belief that the measurements are correlated under real circumstances, whereas compromised measurements disrupt such correlations.

IV. Proposed IDS security against Wormhole Attack

The attacker in WSN is disturbing the actual functioning of routing protocol. The routing protocol are not able to handle the attacker misbehavior because attacker is behaves like as normal node when the sender node is call connection establishment procedure with receiver. The receiver is not known the attacker is generating the fake information of actual route to sender. The sender is not known the reply is generated by wormhole attacker and it trusts the intermediate nodes and starts the data transmission. The wormhole attacker is dropping the all packets that are routed through them. The proposed IDS scheme is designed for identifying the wormhole attack and also protect the network from attack by block the misbehavior activities of mobile nodes. The IDS is based on the data forwarding of intermediate nodes that means the hop count information of each intermediate node. The attacker is never being sender and receiver because their function is not changed. The IDS is actively check the route information or routing of data to each hop count in between sender to receiver if any discrepancy is identified then check the reliability of nodes connected to that link. The whole procedure of detection and prevention from attacker is mentioned in proposed IDS algorithm.

A. Algorithm: Detection and Prevention Wormhole attack

Variable Initialization
M: Set of mobile node
S: Set of senders // M ⊑ S
R: Set of receivers // M ⊑ S
W1 and W2: Wormhole node
Radio Range: 550 Meters
Antenna: Omani directional
Routing Protocol: AODV
IPS: Preventer Node
S broadcast search packet
If (Next Node in range && Node! =Receiver)
{
Receive Routing Packets
Forward Routing Packets to set R
}
Else if (Node ==R)
{
Receive Routing Packets
Send ACK to S node
}
Else
{
Node not in range or unreachable
}
End if
Wormhole node Attack Spreading
S sends data (Sid, Rid, and Route Information)
If (Node R is Intermediate Node && W1)
{
Receive data from incoming node
Forward data only W2 node
}
While (W2 receive data)
{
Selected data capture
Selected data drop
Cannot forward data to next hop }

B. Detection Procedure

Simulated generated data is stored in file.
Analyze behavior of each data
If (Sender ==W1 && next hop ==W2)
{Check W2 forward data or not
If (W2 not forward any data)
{W1 and W2 both is suspicious node}
While (W1 and W2 continuous data capture and not forwarded)
{Both as Attacker}
Prevention Module
In built IPS module in ns-2
Create IPS simulator Setup
If (W1 and W2 both are in IPS node range)
{Detected as wormhole link
IPS node broadcast blocking message of W1 & W2 node
Sender receive message from IPS
}
If (W1 && W2 link in between S to R Link)
{
S change new link eliminate W1, W2 and new path established.
Send data to R node by new path
}
End if
Stop

V. SIMULATION ENVIRONMENT

The simulation is done by NS-2 (Network Simulator-2) Version 2.31[13] which is a discrete event driven simulator developed at UC Berkeley as a part of the VINT project. The goal of NS2 is to support research and education in networking. NS2 is built using object oriented language C++ and OTcl (object oriented variant of Tool Command Language). The NS-2 is the opens source code that easily available. NS2 interprets the simulation scripts written in OTcl. The user writes his simulation as an OTcl script. Some parts of NS2 are written in C++ for efficiency reasons. The wormhole module and the security module is not being the part of simulator setup but it will be built-up after installation.

A. Simulation Parameters

The simulation results of proposed IDS, Wormhole attack and normal routing protocol performance is discussed in this section. The attacker is performing routing misbehaviour and the proposed IDS scheme is block the attacker misbehaviour and improves network performance.

1) NAM Visualization

The NAM (Network Animator) represents the graphic visualization of sensor network nodes. The number of sensor nodes position is clearly visualized. The 15, 36, 37 and 38 are the wormhole nodes 16 and 39 are the IDS nodes. The nodes are clearly visualized the sensing and data packets sending and receiving with Acknowledgement packets. The NAM visualization is mentioned the scenario or actual initial position of sensor nodes and these sensor nodes are communicate with each other for deliver data in network.

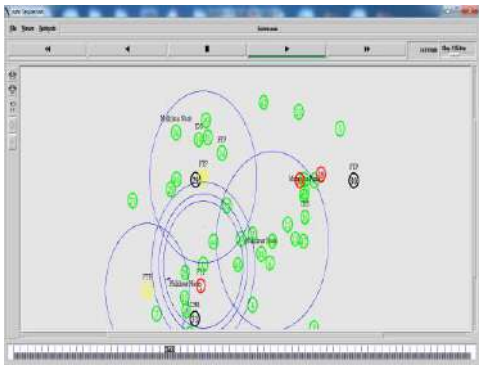

Fig. 5.4 Nam Scenario of nodes

B. PDF Analysis in case of AODV, Wormhole attack and IDS

The packets percentage performance is measured through of Packet Delivery Fraction (PDF). In this graph the PDF analysis in case of normal routing, wormhole attack and secure routing (IDS) is evaluated. The normal routing performance is only evaluated to stint the network performance after applying proposed security scheme. The effect of wormhole attack in network is 20 % at the start of simulation but after that the performance is degrades and reaches to below 1% and maintained it up to end of simulation. The proposed IDS is improves the network performance and provides secure routing. The routing with IDS, the performance of network almost provides 95% PDF, that are improves after applying security scheme against attack. The proposed security scheme is improved the performance in presence of IDS.

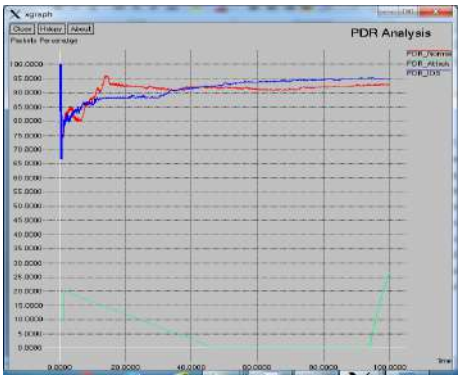

Fig. 5.5 PDR Analysis

1) UDP end packets receiving in case of AODV, Wormhole attack and IDS

The UDP (User Datagram Protocol) is the end to end connection less protocol. The numbers of packets are received at transport layer after routing of data at network layer. The UDP is not reliable protocol and their performance is almost depend on the network conditions, means not heavy loaded, not change topology rapidly and security aspects due to dropping of packets. In this graph the UDP end performance of normal routing, wormhole attack and proposed IDS scheme is measured and recognized that in case of attack the UDP end packets receiving is almost negligible but in case of normal routing and proposed IDS routing the packets receiving is almost equal because of completely block the attacker misbehavior of network. The attacker is easily affected the performance of that protocol but IDS is also provides security by removing routing misbehavior.

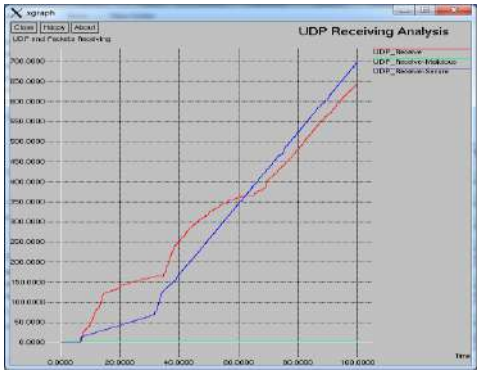

Fig.5.6 UDP Analysis

2) Throughput Analysis in case of AODV, Wormhole attack and IDS

Throughput performance metrics performance is depending on the total number of packets is received at destination in network in per unit of time (like seconds). The better throughput performance is also represents the better data receiving in network. In this graph the throughput performance measurement of normal routing, wormhole and IDS is discussed. The noticeable thing is that the in case of normal routing the throughput is about maximum 2000 packets per second in network but in case of wormhole attack the throughput performance is negligible in network, means up to end of simulation it is about only 10 packets/ sec. but after applying proposed

IDS scheme the throughput is enhance up to 1800 packets/ sec. It means the proposed IDS scheme are definitely improves the network performance and providing the attacker free background of communication in between sender and receiver through intermediate nodes. The variation in throughput is because of selecting the reliable route.

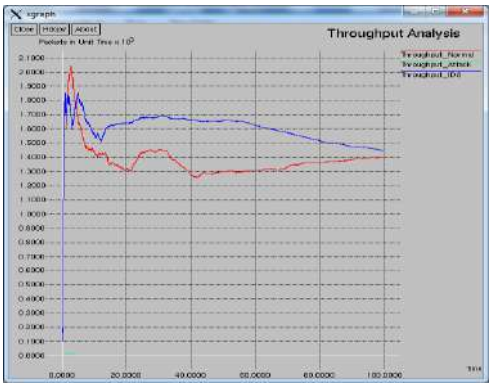

Fig. 5.7 Throughput Performance Analysis

VI. Conclusion And Future Work

Wireless Sensor (WSNs) is eminent from other wireless networks or wired network by many features. First of them is mobile nodes in WSNs can moves freely in the lack of a fixed infrastructure unit. The nodes are mobile and by that the link in between sender to receiver is rapidly changes i.e. the main cause of topology failure. Another one is nodes in WSNs has limited resources such as energy or power, limited bandwidth, and nodes computational power and WSNs have no trusted centralized authority. The proposed IDS method against wormhole attack is not only detect the wormhole attacker but also prevent the network from it. The proposed IDS is improves the routing performance and provides the secure communication. The information of attacker is broadcast to all the nodes that are participating in routing for sending data to destination and genuine nodes are simply deny the request of wormhole attacker if it identified again after block their existence. The attacker infection is very harmful for WSN the routing overhead, throughput and PDF are provides the negligible output but after applying proposed secure IDS scheme the routing packets flooding is minimized with enhancement of performance of PDF and packets receiving. The performance of proposed IDS is supposed to be equivalent to normal routing performance. The characteristic of WSN is a decentralized network and forming dynamic link. The control in nodes movement and security is only possible through some better routing scheme and reliable routing scheme. In future we try to propose the security scheme against jellyfish attack and flooding attack. The attacker identification is not only based on packet loss but also based on heavy packets flooding in WSN.

REFERENCES

[1]. C. Buratti, D. Dardari, R. Verdone, and A. Conti, "An Overview on Wireless Sensor Networks Technology and Evolution", Sensors, Vol. 9, pp. 6869-6896, 2009.
[2]. Theodore S. Rappaport, "Wireless Communication" Prentice Publisher, ISBN 0133755363, January 1994.
[3]. Yongguang Zhang and Wenke Lee, Security in Mobile Ad-Hoc Networks, in Book Ad Hoc Networks Technologies and Protocols, Springer, 2005.
[4]. G. Acs and L. Buttyan, "A Taxonomy of Routing Protocols For Wireless Sensor Networks," Budapest University of Technology and Economics, Hungary, January 2007.
[5]. J. N. Al-Karaki and A. E. Kamal, "Routing Techniques in Wireless Sensor Networks: A Survey," IEEE Wireless Communications, vol. 11, pp. 6–28, Dec, 2004.
[6]. E. M. Royer and C.-K. Toh, "A Review of Current Routing Protocols for Ad hoc Mobile Wireless Networks," IEEE Personal Communications, vol. 6, pp. 46–55, April 1999.
[7]. Raja Waseem Anwar, Majid Bakhtiari, Anazida Zainal,Abdul Hanan Abdullah and Kashif Naseer Qureshiwe, "Enhanced Trust Aware Routing against Wormhole Attacks in Wireless Sensor Networks", IEEE International Conference on Smart Sensors and Application (ICSSA), pp.56-59, 2015.
[8]. Soo-Young Shin, Eddy Hartono Halim, "Wormhole Attacks Detection in MANETs using Routes Redundancy and Time-based Hop Calculation", IEEE International Conference on ICT Convergence (ICTC), pp.781-786, 2012.
[9]. Ravinder Ahuja, Alisha Banga Ahuja, Pawan Ahuja, "Performance Evaluation and Comparison of AODV and DSR Routing Protocols in MANETs Under Wormhole Attack", Proceeding of IEEE Second International Conference on Image Information Processing (ICIIP), pp. 699-702, 2013
[10]. Krontiris, I., T. Dimitriou and F.C. Freiling, "Towards Intrusion Detection in Wireless Sensor Networks", Proceeding of the 13th European Wireless Conference, CiteSeer, 2007.
[11]. Krontiris, I., T. Dimitriou, T. Giannetsos and M. Mpasoukos, "Intrusion Detection Of Sinkhole Attacks In Wireless Sensor Networks" Proceedings of the 3rd International Conference on Algorithmic Aspects of Wireless Sensor Networks, (AAWSN' 28), Springer-Verlag Berlin, Heidelberg, pp: 150- 161, 2008.
[12]. Miss. Prachi S. Moon, Mr. Piyush K. Ingole, "An Overview on: Intrusion Detection System with Secure Hybrid Mechanism in Wireless Sensor Network", International Conference on Advances in Computer Engineering and Applications (ICACEA) pp. 2015.
[13]. http://www.isi.edu/nsnam/ns/.