The International Journal Of Engineering And Science (IJES)
|| Volume || 5 || Issue || 6 || Pages || PP -07-13 || 2016 ||
ISSN (e): 2319 – 1813 ISSN (p): 2319 – 1805

Prevention and Detection of Misbehaving Node in WSN Based On the Intrusion Detection System

S.Deepika[1] , Mrs.M.Jeyaselvi, M.E.,[2]
[1]*ME CSE dept, Agni College of technology, Chennai*
[2]*Sr.Assistant Professor, CSE dept, Agni College of technology, Chennai*

----------ABSTRACT----------
Wireless networks are been used now-a-days. The most paramount fact about wireless network is it is mobile. It is thus utilized in many fields. One of the most paramount applications of wireless networks is Mobile AdhocNETwork (MANET) in which that all the nodes work as both transmitter and receiver. MANETs are utilized in sundry fields like military, industry and emergency recuperation. So it is paramount to have a firsthand erudition about MANETs. But there is a certain drawback in MANETs, in which it becomes prone to malicious attacks very expeditious. To evade such attacks a good intrusion detection system is needed. In this paper, we have proposed a system which can recognize and additionally keep the malicious attacks. The system is named as Enhanced Adaptive Acknowledgments (EAACK). EAACK gives a superior malicious attack than the standard strategies.

Keywords: *Wireless Sensor Network, Watchdog, EAACK, MRA*

Date of Submission: 21 May 2016 Date of Accepted: 06 June 2016

I. INTRODUCTION

In today's life wireless networks are much easier to use rather than wired network. Wireless networks are been used now-a-days. The most paramount fact about wireless network is it is mobile. It is thus utilized in many fields. The ever-incrementing capabilities of these diminutive sensor nodes and it include that sensing, data processing, and communicating, enable the entelechy of Wireless Sensor Networks (WSNs) predicated on the collaborative effort of an astronomically immense number of sensor nodes.

WSNs have a wide range of applications. WSNs are gradually becoming an integral part of our lives. One of the most important applications of wireless networks is Mobile Ad hoc NETwork (MANET) in that all the nodes work as both transmitter and receiver.

WSNs consist of many variants of sensors in which it can able to monitor a wide variety of ambient conditions that include the following: temperature, sultriness, pressure, speed, direction, kineticism, light, soil makeup, noise levels, the presence or absence of certain kinds of objects, and mechanical stress levels on annexed objects. The applications of WSNs can be classified into five categories: Military, environmental, health, home, industry.

II. WSN ARCHITECTURE

The sensor nodes are customarily scattered in a sensor field. The WSN architecture is as shown in Figure 1.1. Each of these scattered sensor nodes has to collect data and back the route data to the sink/gateway and the end-users. By a multi-hop infrastructure less architecture through the sink, data are routed back to the cessation-utilize the sink may communicate with the task manager/end-utilize via the Internet or satellite. Note that there may be multiple sinks/gateways and multiple end-users in the architecture. In WSNs, the sensor nodes have two functionality of being both data and data routers. Hence, communication is performed for two reasons:

- Source function: In order to transmit their packets to the sink, source nodes with event information perform communication functionalities
- Router function: In the multi-hop path to the sink, Sensor nodes participate to forwarding the packets received from other nodes to the next destination.

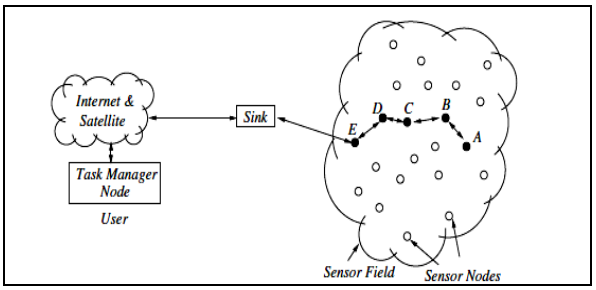


Fig 1: Sensor nodes scattered in a sensor field

III. PROBLEM DEFINITION

Watchdog plan neglects to identify malicious activities with the nearness of the accompanying: 1) ambiguous collisions; 2) recipient impacts (receiver collisions); 3) limited transmission power; 4) false misbehavior report; 5) collusion; and 6) partial dropping. Enhanced Adaptive ACKnowledgement (EAACK) is intended to manage explain the three of the shortcomings of Watchdog plan, in particular, false misbehavior, limited transmission power and receiver collision.

IV. BACKGROUND

As there are a few impediments of MANET such as routing protocol, in routing protocol nodes always think that they are co-agent to each other to exchange information. This assumptions leave attackers to attack the nodes in MANET. IDS should be added in MANET for security level. In this, we mainly describe an existing system, namely, EAACK (Enhanced Adaptive ACKnowledgment).

EAACK- In these, EAACK is intended to overcome three of the three shortcomings of Watchdog methodology, as, false misbehavior, limited transmission power, and receiver collision [3].

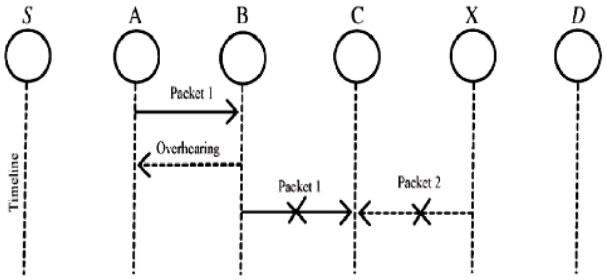


Figure 2: Receiver Collision

Node A sends Packet 1 to node B, it endeavors to overhear if node B forwarded this packet to node C; meanwhile, node X is forwarding packet 2 to node C. due to a collision between Packet 1 and Packet 2 at node C, in such case node A overhears that node B has prosperously, forwarded Packet 1 to node C, but failed to detect that node C did not receive this packet [3].

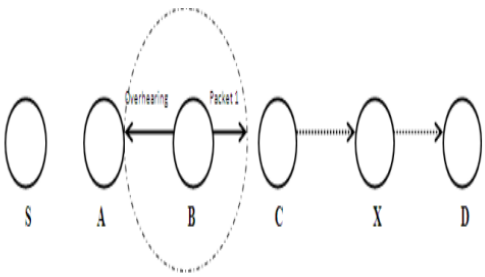


Figure 3: Limited Transmission Power

Node B purposefully limits its transmission power. Presently, node A can hear that node B has sent packet1 to node C. However, [3] as node B has prevented its transmission power node A can't hear whether node c has gotten packet1 or not.

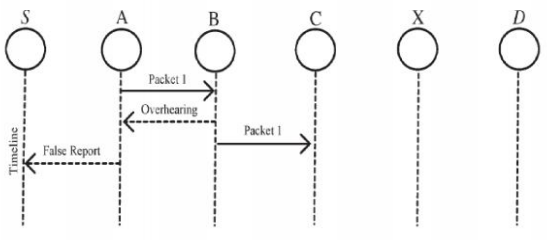


Figure 4: False Misbehavior Report

Node A sends Packet1 to Node B. As node B gets Packet1 it quickly sends Packet1 to node C. Presently Node A becomes more acquainted with that Node B has effectively sent the packet to Node C, still Node A sends false answer to the source node or past node that node B is getting into misbehaving. This is known as false misbehavior report [5].

ACK:

ACK is fundamentally a terminus-to-end acknowledgment scheme. In this, first node has to send Packet to second node, and that second node has to give back acknowledgment to the first node [3]. If within duration the second node doesn't send back acknowledgment then again that Packet is being send.

S-ACK:

S-ACK is similar to TWOACK. In S-ACK three successive nodes work in a gathering to distinguish acting misbehaving nodes. For each three successive nodes in the route, the third node is required to send an S-ACK acknowledgment packet to the primary node. In TWOACK scheme[3], the source node immediately trusts the misbehavior report sent by the other intermediate nodes, in EAACK there is a mode named MRA, which first confirm whether the node is misbehaving or not, and then takes the decision of declaring it malicious.

MRA:

MRA plan is intended to determine the shortcoming of watchdog. Watchdog neglects to identify the false misbehavior report [2].

When the source node gets the report of false misbehavior, at that time the source node sends the report to MRA mode. Then in the MRA mode, another route is assigned through its local base knowledge and the same packet is sent again to the destination, but through different route. When the packet reaches destination, MRA checks whether the packet is reached its destination or not through its local knowledge base. If destination has already received the same packet before, then MRA concludes that it is a false report and whichever node generated this report is marked malicious. If the packet has reached its destination for the first time then the misbehavior report is trusted and accepted. Because of this plan EAACK has outlined, it is equipped for recognizing malicious nodes [3].

V. RELATED WORKS

A. Existing system

In the Existing system, COCOWA as a collaborative contact-predicated watchdog to reduce the time and amend the efficacy of detecting selfish nodes, reducing the deleterious effect of selfish node (false positives, false negatives) and malicious nodes. COCOWA is predicated on the diffusion of the known positive and negative detection[1].The diffusion module transmits and processes the positive and negative detection when a contact occurs between two collaborative nodes [8].

The utilization of watchdog is a well-kenned mechanism to detect selfish nodes. The detection process performed by watchdog can fail, generating false positives and false negatives that can induce to incorrect operations. When detecting selfish nodes relying on local watchdog alone can lead to poor performance in term of precision and haste. This is especially consequential on networks with sporadic contacts. Collaborative contact-predicated watchdog as a collaborative approach predicated on the diffusion of local selfish nodes awareness, so that information about selfish nodes is expeditiously propagated.

Watchdog is capable of detecting malicious nodes rather than links. Watchdog that aims to improve the throughput of network with the presence of malicious nodes. In fact, the Watchdog scheme consists of two parts, namely, Watchdog and Pathrater [4]. Watchdog serves as IDS for MANETs. It is responsible for detecting malicious node misbehaviors in the network. Watchdog detects malicious misbehaviors by promiscuously listening to its next hop's transmission. If a Watchdog node overhears that its next node fails to forward the packet within a certain period of time, it increases its failure counter. Whenever a node's failure counter exceeds a predefined threshold, the Watchdog node reports it as misbehaving [3]. In this case, the Pathrater cooperates

with the routing protocols to avoid the reported nodes in future transmission. The Watchdog scheme fails to detect malicious misbehaviors with the presence of the following: 1) ambiguous collisions 2) receiver collisions 3) limited transmission power 4) false misbehavior report 5) collusion and 6) partial dropping [6].

Disadvantages:

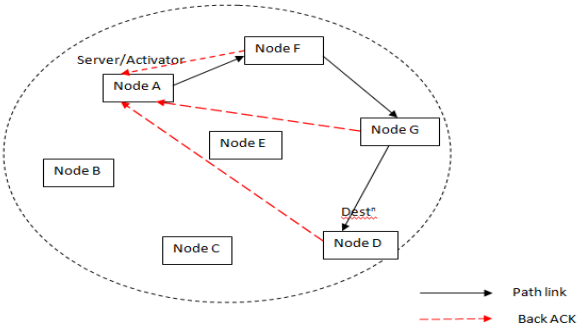
- Attacker detection process is difficult on existing system.
- High overhead due to the data transmission from source to destination.
- The data transmission process takes much time on existing system.

B. Proposed System

In this paper, we have proposed a framework/system which can recognize and in addition keep the malicious attacks. The framework is named as Enhanced Adaptive ACKnowledgment (EAACK). EAACK gives a better malicious-behavior-detection than the traditional approaches. EAACK comprises of three major parts, in particular, ACK, secure ACK (S-ACK), and misbehavior report authentication (MRA). ACK is essentially an end to-end affirmation plan. In this, first node needs to send Packet to second node, and that second node needs to give back affirmation to the first node. MRA plan is intended to determine the shortcoming of Watchdog. Watchdog neglects to recognize the false misbehavior report [5].
At the point when the source node gets the report of false misbehavior, around then the source node sends the report to MRA mode [3].

VI. SYSTEM ARCHITECTURE

The system architecture as shown in the figure 5.



Node A needs to send packets to Node D through node F, G. Thus enacted way is A-F-G-D. At the point when packet is sent from Node A to Node F back acknowledgment is sent to Node A which is a server node. At the point when the packet is sent to Node G back acknowledgment is sent straightforwardly to Node A. At the point when the packet comes to the destination that is node D will send an acknowledgment to node A that the packet is reached [3].

Module Description

In this project, there are four modules. The following are the modules and their brief description.

A. Network Formation

The single-duplicate directing instrument, for example, First Contact routing protocol, and we expect the correspondence scope of a mobile node is limited. In this way an information sender out of destination node's correspondence extent can just transmit packetized information by means of a sequence of intermediate nodes in a multi-hop manner. Illustration node A has bundles, which will be conveyed to node C. Presently, [4] if node A meets another node B that could forward the packets to C; A will repeat and forward the packets to B. From there on, B will forward the packets to C when C arrives at the transmission range of B. The First Contact Routing Protocol can be utilized to find the way. In the system the node have some coverage and mobility. The neighbour nodes are changed in each node based on its mobility. The route discovery is based on the source and destination, nearest node can be chooses to forwarder.
It is one of several demand-driven (or on-demand) protocols that are in presence today. Consequently, the protocol is invoked only when a node (host) has information to transmit. Route discovery mechanism is invoked only if a route to destination is known. Every node keeps up a routing table that contains data about the achieving destination nodes and this node goes about as both a host and a routing node. It is a reactive protocol. It handles congestion problem.

B. Watchdog Mechanism

Watchdog is additionally an IDS for MANETs. Watchdog was intended for identifying malicious node misbehavior in the system [2]. In Watchdog next hop transmission is utilized for recognizing malicious nodes. Watchdog listens to its next hop transmission. If a Watchdog node overhears the next node fails to forward the packet for a certain period of time [3].

The basic function of the intrusion detection system is watchdog. In watchdog, it can distinguish andpreventing the misbehaving node (selfish and malicious node). Presents a COCOWA, which could dispatch the collaborative contact predicated watchdog for the objective node and judge it by collecting the sending history proof from its ups and downstream nodes [1]. At that point COCOWA could punish compensate the node predicated on its comportments. To facilitate improve the execution of the proposed collaborative inspection scheme.

C. Cluster Formation

The cluster formation is each gathering of node is framed together and arranged in one Group. The principle reason for cluster formation is reduce the Transfer Rate and allotment of gathering into subgroups lastly one leader will be chosen. For the Selection of Group different strategy will be utilized.

D. ACK and S-ACK Scheme:

ACK is essentially an end-to-end affirmation plan [6]. In this, first node needs to send Packet to second node, and that second node needs to give back affirmation to the first node. On the off chance that inside time period the second node doesn't send back affirmation on the other hand that Packet is being send. S-ACK plan is an enhanced version of TWOACK. In S-ACK three successive nodes work in a gathering to identify getting into misbehaving nodes. For each three consecutive nodes in the route, the third node is required to send an S-ACK confirmation group to the primary node. In TWOACK arrangement, the source node rapidly trusts the misbehavior report sent by the intermediate nodes. The intention of introducing S-ACK mode is to detect misbehaving nodes in the presence of receiver collision or limited transmission power [2].

VII. ANALYTICAL EVALUATION

In this paper we focus on those parameters that clearly affect performance. First, we study the global performance of our approach considering the collaborative issues. In Figure 2 and 3 it's shows that comparison of IDS (Existing) and Secure IDS(proposed).

Fig 6: Performance evaluation of data packet loss

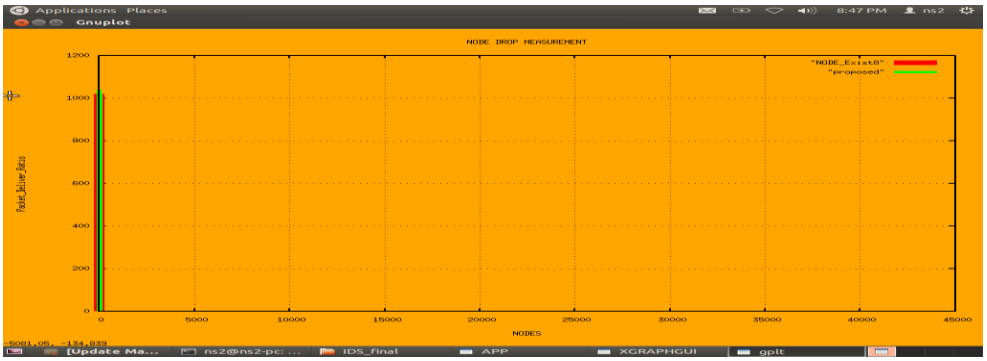


Fig 7: Performance of node packet delivery

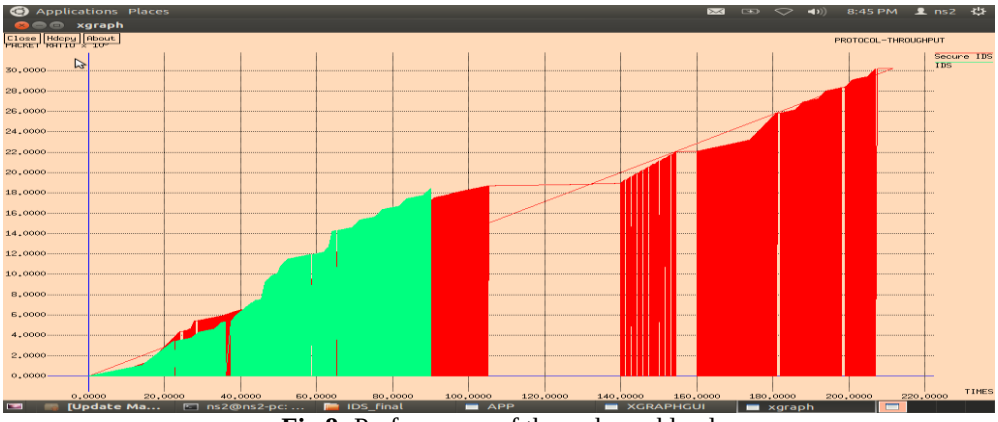


Fig 8: Performance of through workload

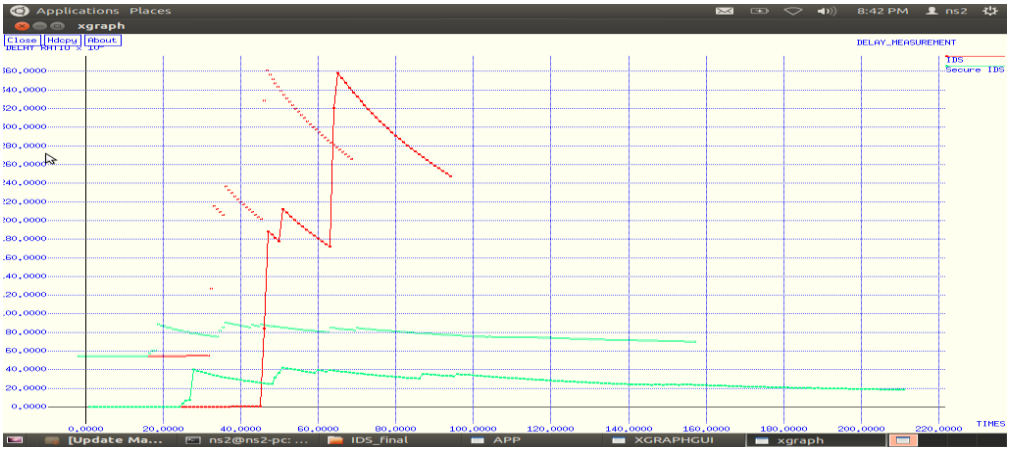


Fig 9: Performance of delay ratio

Fig 10: Performance of Source signal strength

VIII. CONCLUSION AND FUTURE WORK

The most discussed field when MANETs are concerned is Intrusion Detection System Intrusion detection system which concentrates on distinguishing and preventing many attacks in the system which can be harmful. At the point when security issues are seen then packet dropping and hacking are significant worries in MANETs. We have given an IDS named EAACK with a few new techniques for avoidance of attacks included.There are a few elements in the system:

1. This system has a capable attack control, which is one of the essential conditions to ensure the information security.
2. Once the activator characterizes the keys to the nodes, the need will be produced naturally. Also, each record would be put away at the activator database.

We can broaden the extension for various attacks in future some of which could be different attacks in DOS like black hole attack or even spoofing. Watchdog has a sum of six shortcomings of which three are taken care of with this framework the other three could be taken care of in future.

REFERENCES

[1]. Enrique Hern´andez-Orallo, Manuel D. Serrat, Juan-Carlos Cano, Carlos T. Calafate, Pietro Manzoni., Jun. 2015."CoCoWa: A Collaborative Contact-Based Watchdog for Detecting Selfish Nodes" IEEE Syst. J., vol. 14, no. 6, pp. 236–248.

[2]. Miss. Kalyani, S. Ghodake, Miss. Madhura J. Bade, Miss. Poonam A. Pange, Mr. Amit D. Bansode, "EAACK—A Secure Intrusion-Detection System for MANETs", IJISET, Engineering & Technology, Vol. 2 Issue 3, March 2015.

[3]. Poonam Joshi, PoojaNande, AshwiniPawar," EAACK- A Secure Intrusion Detection and Prevention System for MANETs", IEEE, 2015 International Conference on Pervasive Computing (ICPC).

[4]. PawarPriyanka, Hashmi S.A," Security Enhanced Adaptive AcknowledgmentIntrusion Detection System", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (5), 2015, 4812-4817.

[5]. M.Geetha, N.Senthilkumar," Misbehavior Report Authentication IntrusionDetection System in MANETs", IJIRSE, ISSN (Online) 2347-3207, 2014.

[6]. K.Chinthanaichelvan, T.Sangeetha, V.Prabakaran, D.Saravanan,"EAACK-A Secure Intrusion Detection System for MANET", An ISO 3297: 2007, Vol. 2, Issue 4, April 2014.

[7]. EhsanAmiria, Hassan Keshavarzb, HosseinHeidari., May. 2014. "Intrusion Detection Systems in MANET", IEEE Syst. J., vol. 129, no. 6, pp. 453–459.

[8]. MominKashifMukhtar," A Collaborative Contact-Based Watchdog forDetecting Selfish Nodes in Cooperative MANET", IJRET, Volume: 03 Issue: 11, Nov-2014.

[9]. E. Hernandez-Orallo, M. D. Serrat, J.-C. Cano, C. M. T. Calafate, and P. Manzoni.,May 2012. "Improving selfish node detection in MANETs using a collaborative watchdog," IEEE Comm. Lett., vol. 16, no. 5, pp. 642–645.