A Comparative Study of EAACK Based Security Mechanism for MANETs

Brijal J. Patel[1], **Krunal Panchal**[2]

[1]Research Scholar, Information Technology Department, LJ Institute of Engineering & Technology, Gujarat, India

[2] Assistant Professor, Information Technology Department, LJ Institute of Engineering & Technology, Gujarat, India

ABSTRACT

A Mobile ad hoc network (MANET) is an autonomous system of wireless mobile nodes that can be dynamically setup anywhere and anytime. MANET differs from cellular networks or conventional wired networks as there is no centralized access point [9]. MANET allows multi-hop communication among nodes that are not in direct transmission range through intermediate nodes. Nodes are free to move randomly thus form arbitrary network topology. There is various type of attacks MANETs. Providing security against the intruder is a challenging task in MANET. *In this paper, we present the Modified Enhanced Adaptive Acknowledgment (EAACK) based Intrusion Detection system that is used to mitigate the attacks. And Increase a performance or Packet delivery ratio.*

Keyword: - *Watchdog; Enhanced Adaptive Acknowledgement (EAACK); Digital Signature; IDS; Clustering*

1. INTRODUCTION

A mobile ad hoc network (MANET) is a one of the wireless method. The device are moving in randomly different directions and communicating with one to other within each nodes communication range. To extend the nodes communication range , the other nodes in the network act as router .Thus the communication may occurring via multiple intermediate nodes between source and destination.[6]MANETs have a wide range of applications , specifically in military operations and emergency and disaster relief efforts.

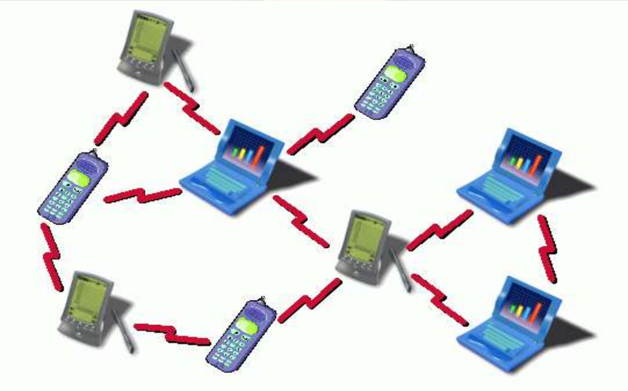

Fig.1: Mobile Ad-hoc Network[10]

MANET is a collection of mobile nodes equipped with both a wireless transmitter and a receiver that communicate with each other via bidirectional wireless links either directly or indirectly[11].One of the major advantages of wireless networks is its ability to allow data communication between different parties and still maintain their mobility. However, this communication is limited to the range of transmitters. This means that two nodes cannot communicate with each other when the distance between the two nodes is beyond the communication range of their own. MANET solves this problem by allowing intermediate parties to relay data transmissions. This is achieved by dividing MANET into two types of networks, namely, single-hop and multihop.[7]

The open network and remote distribution method of MANETS make it vulnerable to various type of attacks. The nodes environmental protection , malicious attackers can easily capture and compromise nodes and make attacks. most of routing protocols in MANETs assume that every node in the network behave cooperatively with other nodes and presumably not malicious attackers can easily compromise MANETs by inserting malicious or no Cooperative node into the network. An intrusion detection systems, which is used to detect and mention an attack after it is accrued. This system are very important to MANET's security.[3][9]

In this paper, we focus on Enhanced Adaptive Acknowledgment(EAACK) scheme which overcome issues present in WATCHDOG such as Ambiguous collision, Receiver collision, Limited transmission Power, False misbehavior report, collusion, partial dropping.

2. INTRUSION DETECTION SYSTEM FOR MANETS:

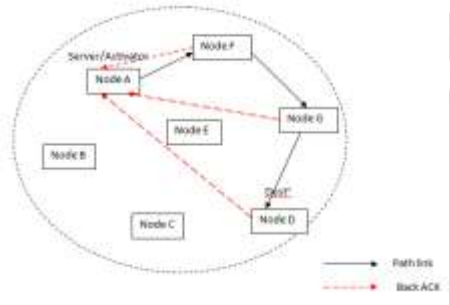

Fig.2: Intrusion Detection System[1]

In previous intrusion detection system, acknowledgments were sent to the previous nodes and then from previous nodes to the server, this used to make intrusion detection system more complex and time required to reach acknowledgment to the server was more. Time complexity of the given system is less than previous IDS.

In above Fig 2. Node A has to send packets to Node D through nodes F, G. Therefore activated path is A-F-G-D. When packet is sent from Node A to Node F back acknowledgment is sent to Node A which is a server node. When the packet is sent to Node G back acknowledgment is sent directly to Node A. When the packet reaches the destination i.e. Node D it will send an acknowledgment to Node A that the packet is reached.[1]

2.1 WATCHDOG

Watchdog was designed for detecting malicious node misbehavior in the network. In Watchdog next hop transmission is used for detecting malicious nodes. Watchdog listens to its next hop transmission. If a Watchdog node overhears that its next node fails to forward the packet for a certain period of time, it increases its failure counter. Whenever a node's failure counter exceeds a predefined threshold value, the Watchdog node reports it as misbehaving. 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 [3].

2.1.1 AMBIGUOUS COLLISION:

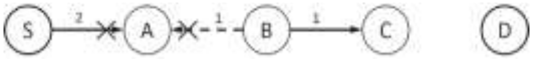

Fig.3: Ambiguous Collisions[2]

This prevents one node from overhearing packet transfer from other nodes. Considering scenario in figure 1, the collision is occurred at node A because node A overhears B for packet transmission and at the same time it receives next packet from S. At this instance A may conclude B as misbehaving node as it fails to overhear B's transmission. Here node B is wrongfully declared as misbehaving node by A [2].

2.1.2 RECEIVER COLLISION:

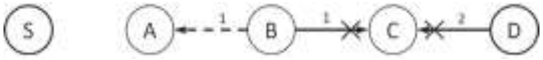

Fig.4: Receiver Collisions[2]

In the receiver collision problem,(refer figure 4) a node (node A in our case) can only tell whether neighboring node (node B) sends the packet to its neighbor (node C) which is 2 hop away from the initial node (node A), but it cannot tell if node (C) which is 2 hop away receives it. Considering example in figure 2, If a collision occurs at C when B first forwards the packet, A can only see B forwarding the packet and assumes that C successfully receives it. The node B can skip retransmitting the packet to C. In this case B is selfish and saves its resources. And B could also intentionally cause collision at C. Here node B is taking malicious actions and wastes it's battery as well as CPU time[2].

2.1.3 LIMITED TRANSMISSION POWER:

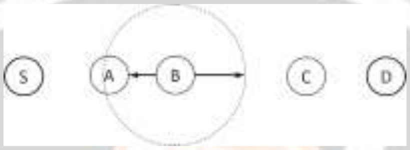

Fig.5: Limited Transmission Power[2]

A node could limit its transmission power, such that the signal can be overheard by the previous node and not by the true recipient. For this purpose the misbehaving node keeps track of the transmission power required to reach each of its neighboring nodes [2].

2.1.4 FALSE MISBEHAVIOUR REPORT:

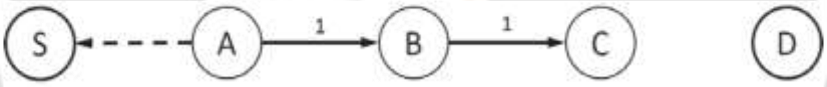

Fig.6: False Misbehavior Report[2]

Another issue can occur when a node reports legitimate node as misbehaving node. In this case, a malicious node falsely claims that some nodes in the path are acting maliciously. For instance, node A could report that node B is misbehaving by not forwarding packets when in fact it is, as shown in figure 4. Node B is listed as misbehaving node as reported by A [2].

2.1.5 COLLUSION:

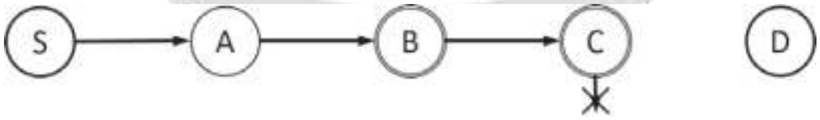

Fig.7: Collusion[2]

Multiple nodes in collusion can mount a more sophisticated attack. In figure 5, node B and C cooperatively launches an attack by dropping packets without getting caught by neighboring nodes. In this case, B and C are misbehaving nodes. Here B forwards packet to C and A overhears it. But later C drops packets forwarded by B, which cannot be overheard by A. This is how colluding nodes remain undetected [2].

2.1.6 PARTIAL DROPPING:

Here a misbehaving node may drop packet at very lower rate. In watchdog the threshold value for packet dropping is maintained to identify node as behaving node. So the malicious node will keep its packet dropping count such that it will not cross the threshold value [2].

3. EAACK SCHEME:

EAACK consists of three major parts, namely, ACK, secure ACK (S-ACK), and misbehavior report authentication (MRA). But improved EAACK consist one more mode that is Special mode.[2]

3.1 ACK:

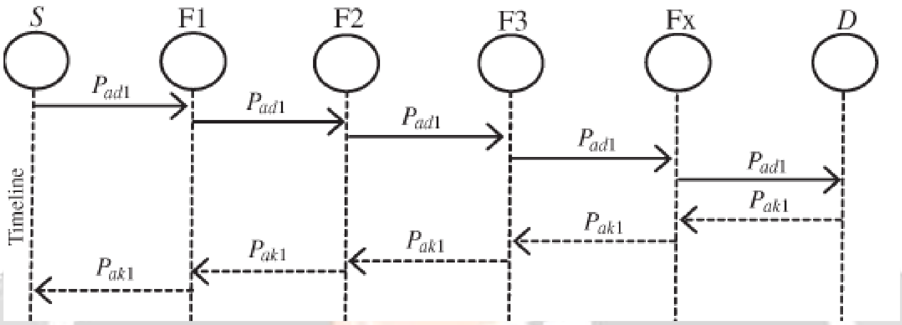

Fig.8: ACK Scheme[8]

ACK is basically an end-to-end acknowledgment scheme. It acts as a part of the hybrid scheme in EAACK, aiming to reduce network overhead when no network misbehavior is detected.[1] In Fig. 8, in ACK mode, node S first sends out an ACK data packet *Pad*1 to the destination node D.

If all the intermediate nodes along the route between nodes S and D are cooperative and node D successfully receives *Pad*1, node D is required to send back an ACK acknowledgment packet *Pak*1 along the same route but in a reverse order. Within a predefined time period, if node S receives *Pak*1, then the packet transmission from node S to node D is successful. Otherwise, node S will switch to S-ACK mode by sending out an S-ACK data packet to detect the misbehaving nodes in the route.

3.2 SECURE ACK (S-ACK):

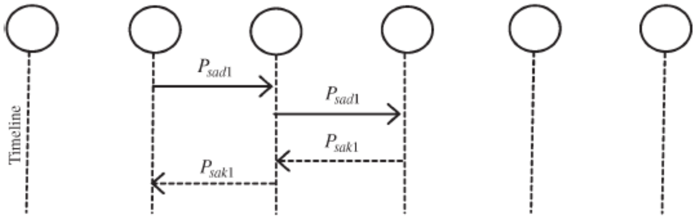

Fig.9: S-ACK Scheme[8]

The S-ACK scheme is an improved version of the TWOACK scheme proposed by Liu *et al*. The principle is to let every three consecutive nodes work in a group to detect misbehaving nodes. For every three consecutive nodes in the route, the third node is required to send an S-ACK acknowledgment packet to the first node. The intention of introducing S-ACK mode is to detect misbehaving nodes in the presence of receiver collision or limited transmission power. As shown in Fig. 6, in S-ACK mode, the three consecutive nodes (i.e., A, B, and C) work in a group to detect misbehaving nodes in the network. Node A first sends out S-ACK data packet *Psad*1 to node B. Then, node F2 forwards this packet to node C. When node C receives *Psad*1, as it is the third node in this three-node group, node C is required to send back an SACK acknowledgment packet *Psak*1 to node B. Node B forwards *Psak*1 back to node A. If node A does not receive this acknowledgment packet within a predefined time period, both nodes B and C are reported as malicious. Moreover, a misbehavior report will be generated by node F1 and sent to the source node S.

Nevertheless, unlike the TWOACK scheme, where the source node immediately trusts the misbehavior report, EAACK requires the source node to switch to MRA mode and confirm this misbehavior report. This is a vital step to detect false misbehavior report in our proposed scheme.

3.3 MISBEHAVIOR REPORT AUTHENTICATION (MRA):

The MRA scheme is designed to resolve the weakness of Watchdog when it fails to detect misbehaving nodes with the presence of false misbehavior report. The false misbehavior report can be generated by malicious attackers to falsely report innocent nodes as malicious. This attack can be lethal to the entire network when the attackers break down sufficient nodes and thus cause a network division. The core of MRA scheme is to authenticate whether the destination node has received the reported missing packet through a different route. To initiate the MRA mode, the source node first searches its local knowledge base and seeks for an alternative route to the destination node. If there is no other that exists, the source node starts a DSR routing request to find another route. Due to the nature of MANETs, it is common to find out multiple routes between two nodes.[1][2]

By adopting an alternative route to the destination node, we circumvent the misbehavior reporter node. When the destination node receives an MRA packet, it searches its local knowledge base and compares if the reported packet was received. If it is already received, then it is safe to conclude that this is a false misbehavior report and whoever generated this report is marked as malicious. Otherwise, the misbehavior report is trusted and accepted.[8]

3.4 SPECIAL MODE:

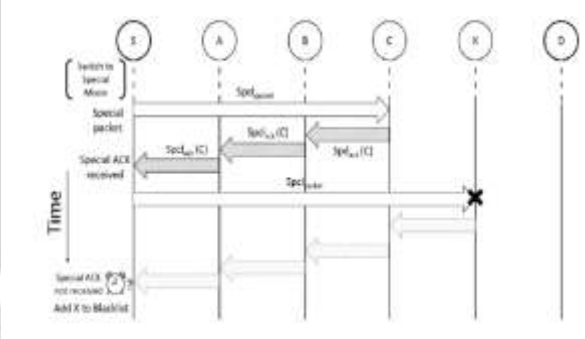

Fig.10: Special Mode[2]

In this mode, as source has received NACK from a trusted node, so up to that node the path is safe. And now we know that the misbehaving node is one of the nodes who are within two hop range of last trusted node. So to identify that, Source sends Special Packet directly to next node of the node which has sent an NACK and waits for Special Acknowledgement packet from it. If source does not receive any Special Acknowledgement within predefined time, then it will add that node to the blacklist; Otherwise the second node is the misbehaving node. But we cannot directly blacklist any node without verifying, so the same procedure is repeated for the node which is two-hop away from the sender of NACK packet.[2]

Blacklist:

This is a list containing misbehaving nodes as shown in table I. It contains information about nodes such as Serial number, Node ID, Duration. Node ID is an ID of malicious node, and Duration is for how much time the node is declared as misbehaving node. This black list will be updated and shared with other nodes in the network periodically.[2]

4. DIGITAL SIGNATURE:

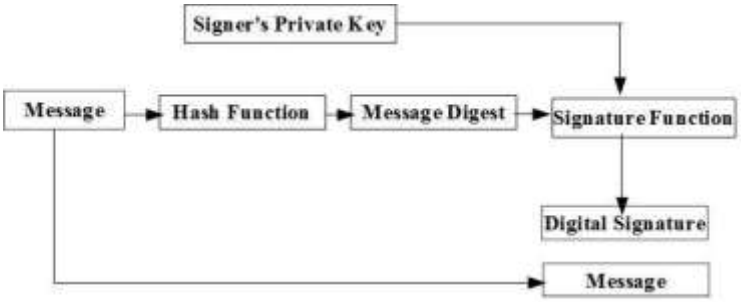

Fig.11: Digital Signature[4]

Digital Signature nothing but the part of cryptography. Cryptography is nothing but the mathematical technique which is used for providing security to information such as affinity ,purity, entity validation, data root authentication.[5]

The security in MANET is illustrated as a mixture of processes, procedures ,systems utilized to confirm affinity, validation, purity, accessibility and non refusal. It is mostly useful scenario to make sure the affinity, purity, non refusal for MANET. To confirm the accuracy of digital signature, the massage is first sent to hash function or in case the message is valid data means it directly send to the messages and the hash function is processed and after that it sends to the message digest, validity of message is checked by message digest after all these process it can be then sent to signature function, it check the signature whether its private key or public key.[4][5]

Digital signature can have two categories:

Digital signature including appendix : In that process the actual message is needed in the signature verification form. example: DSA).

Message repossession with Digital Signature : This type of technique only demands the signature itself in verification process rather than having other information.

5. CLUSTERING:

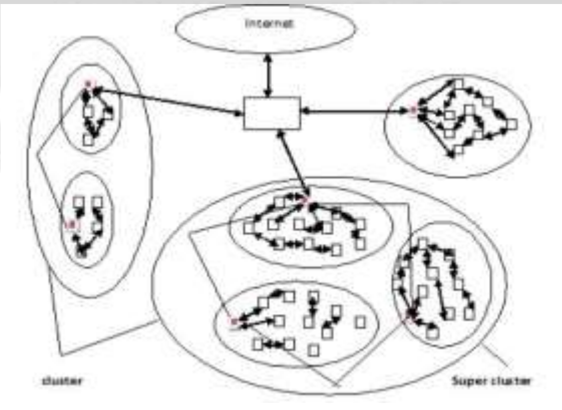

Fig.12: Hierarchical Clustering[4]

If large count of host are involved in network then hierarchical clustering of host in MANET is feasible solution to improve the performance. There are some algorithms like Destination Sequenced Distance-Vector (DSDV), Ad-hoc On-Demand Distance Vector (AODV) and Dynamic source Routing(DSR) which are works for less count of host. When the network is larger, then clustering of hosts and also using distinct algorithm like routing algorithms between and within cluster can be a better solution. The main aim behind this approach is location property. If topology within cluster is change, then only those nodes are get inform which are present in cluster. This approach hides all the small details in cluster. From time to time basis each and every node within a cluster gets some information about the topology.

Combination of cluster forms super cluster etc, constructing a larger hierarchy. With the use of this approach more than one node can acts as cluster heads, also show a router for all traffic to/from the cluster.

Fig. 11 shows ad-hoc network which get interconnected to internet through base station. The base terminal transfer the information to and from cluster heads.

Now a days many hierarchical algorithm are used.

1) Agglomerative: This is ‘bottom up’ scenario where nodes gets start from its own cluster and merging of cluster pair is done and move up the hierarchy.

2) Divisive: This is ‘top-down’ scenario where, in one cluster all obviations are gets began, and periodically perform the splitting , as one goes down the hierarchy. Bottom up scenario mainly utilized in MANET’s during the clustering is get completed.[4]

6. CONCLUSION AND FUTURE WORK

In this paper, EAACK and IDS system for prevent and detect malicious attacks. Watch dog has a total of six weaknesses such as ambiguous collisions, receiver collisions, limited transmission power, false misbehavior report, collusion, and partial dropping in which three are handled with this system such as receiver collisions, limited transmission power, false misbehavior report. EAACK gives a better malicious-behavior-detection than the traditional approaches. In EAACK special mode help to detect actual malicious node. Digital signature is part of cryptography that gives confidentiality, data integrity, entity authentication and data origin authentication. This gives an optimal solution for EAACK scheme and to reduce the network overhead in the case of authentication. Clustering routing algorithm provide security which find the secure routing and also provides some cryptography algorithms. In future work to solve other attacks and also work on security with energy efficient scheme for MANETs.

7. ACKNOWLEDGEMENT

I would like to express my sincere gratitude to Prof. Krunal Panchal, LJ Institute of Engineering & Technology, Ahmadabad, under whose supervision this research has been undertaken. I would also like to thank all other faculty members of Information Technology Engineering department of LJ Institute of Engineering & Technology who directly or indirectly kept the enthusiasm and momentum required to keep the work towards an effective research alive in us and guided in their own capabilities in all possible ways.

8. REFERENCES

[1] Poonam Joshi, Pooja Nande, “EAACK – A secure intrusion detection and prevention system for MANETs” 978-1-4799-6272-3/15@2015 IEEE International Conference on Pervasive Computing (ICPC).

[2] Ashish Patil,Nilesh Marathe,**“**Improved EAACK scheme for detection and isolation of a malicious node in MANET**”,**978-1-4673-9223-5/15@2015 IEEE International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT).

[3] Dipamala Nemade, Ashish T. Bhole,“Performance evaluation of EAACK Ids using AODV and DSR routing protocols in MANET”,978-1-4673-9563-2/15@2015 IEEE International Conference on Emerging Research in Electronics, Computer Science and Technology.

[4] Deore Suvarna , Erande Pallavi, “Acknowledgement security for MANET using EAACK”,978-1-4673-7910-6/15@2015 IEEE International Conference on Green Computing and Internet of Things (ICGCIoT).

[5] Elizabeth Sherine.M, “Effective intrusion detection method for MANETs Using EAACK”, 978-1-4799-7075-9/15@2015 IEEE International Conference on Circuit, Power and Computing Technologies [ICCPCT].

[6] G.Indumathi, S.Sakthivel, “Securely Detecting An Intruders In MANETs System”, 978-1-4799-3834-6/14@2014 IEEE.

[7] M. Jegannath, Mr. P. Sivakumar, “A Robust Trust Aware Secure Intrusion Detection in MANET ”, 978-1-4799-3834-6/14@2014 IEEE.

[8] G.Girija, Dr.M.G.Sumithra, “A MODIFIED EAACK-INTRUSION DETECTION SYSTEM FOR MANETs”, 978-1·4799-3448-5/13@2013 IEEE International Conference on Advanced Computing (ICoAC).

[9] Preeti Sachan, Pabitra Mohan Khilar, “Securing AODV Routing Protocol in MANET Based on Cryptographic Authentication Mechanism”, International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.5, Sep 2011.

[10] Ux1.eiu.edu,. N.p., 2007. Web. 21 Oct. 2016(11:15:25).

[11] Google.co.in,. 'Mws_Gen_Int_Ppt_manet.Ppt'. N.p., 2008. Web. 23 Aug. 2016(11:20:20).