RESEARCH ARTICLE OPEN ACCESS

An Comparative study and evaluation on performance of Intrusion Detection Schemes in MANET

Deepika Goyal[1] , Mr. Deepak Kumar Xaxa(Assistant Professor)[2]

Computer Science & Engineering, School of Engineering & IT
MATS University, Aarang, Raipur (C.G), India

Abstract:

Mobile Adhoc Network (MANET) is a wireless communication mechanism. It is a collection of mobile nodes that have a dynamic infrastructure, due to its dynamic nature every node acts as a transmitter and receiver. MANET is capable of self configuring ,this unique feature make it ideal in various application like military use and emergency situation like medical ,natural disaster etc. Due to open medium and wide distribution of node, MANET is susceptible to malicious attackers thus there is a need to develop IDS (Intrusion Detection System) in order to protect MANET from attacks as security is of highest concern. However many IDS has been proposed by researchers to detect malicious (misbehaving) node in mobile adhoc network .All IDS will demonstrate its performance in terms of routing overhead and packet delivery ratio. The main objective of this paper is to observe and analyze the performance of Watchdog, TwoAck, AACK and EAACK. The result will provide positive performances against malicious node detection, however EAACK will demonstrate higher malicious detection rate in certain circumstances as compares to other IDS while does not greatly affecting the network performance.

Keywords:-**EAACK, Digital signature, MANET, Intrusion Detection system**

INTRODUCTION:

In the current era, Wireless network is of growing interest over wired network because of its mobility and scalable nature as well as reduced cost and improved technology. MANET is a collection of mobile nodes forming a network that has a dynamic infrastructure. MANET is a self configuring and self organizing network where every node acts as a transmitter and receiver connected by a bidirectional links[1]. MANET is of two types: Single hop network in which nodes communicate directly with each other in same communication range and multihop network in which node depends on neighbor node for forwarding packet to destination node beyond the communication range. This advantage accomplishes the need of Wireless network that is allowing the data communication between nodes and still remaining mobile in nature. The nodes while communicating follows dynamic topology and are thus free to move randomly[2]. As Manets does not need a fixed and centralized infrastructure as well as it configures its dynamic network quickly with minimal configuration thus it is used in various areas like military conflict, intelligent transportation system as well as in emergency circumstances.

It is also used in areas where infrastructure is unfeasible to install in scenarios like natural disasters and medical emergency situation.[3][4].Due to its unique characteristics, MANET is widely implemented in the industry[5].

Due to open medium and dynamic distribution of nodes, MANET is susceptible to various types of attack such as passive attack(Eavesdropping) and active attack(Spoofing,

Dos.)[6].Thus to protect MANET from Attacks, Intrusion Detection System needs to be developed as security is of highest concern. Different methods have been proposed in order to mitigate routing misbehavior in MANET.

One of the most important technique is Watchdog that detects malicious node with the improvement of throughput. Initially these malicious node agrees to forward packets but fails to do and drop packets[8]. In this scheme two tools are used watchdog that detects misbehavior node by overhearing and pathrater that cooperates with the routing protocols to avoid malicious node in future.

In order to overcome limitation of watchdog TwoAck IDS have been proposed which detects malicious link rather than nodes[9]. It works for three consecutive

nodes by sending acknowledgment for every data packet. This improves malicious detecting rate but with significant amount of network overhead due to ACK[10].Thus new scheme has been proposed to reduce network overhead but with same throughput or better PDR on average is AACK.

AACK is a combination of ACk and TwoAck and works over DSR. It also detects misbehaving link and does not isolate misbehaving node completely. However it provides better network performance as compared to TwoAck but still cannot detect malicious node in presence of forged ACk and false misbehavior report[10].To solve this problem a new IDS has been developed adopting digital signature called EAACK.

To mitigate the effects of malicious node in MANETs, many researchers provided proactive security approaches like cryptography and authentication in EAACK[11]. It solves the problem of above IDS and provides better network performance in presence of false misbehavior report and forged ACK as compared to watchdog, TwoAck and Aack. However routing overhead is also maintained, but if malicious node increases, RO rises rapidly due to digital signature.[12].

The rest of the paper is organized as follows. Section 2 presents the problem definition that describes need of IDS. Section 3 presents the different methodology for detecting malicious nodes. Section 4 will demonstrate the result that will help us to analyze the performance of network. Finally paper is concluded with section 5 along with result discussion.

I. PROBLEM DEFINITION

Due to open medium and wide distribution of nodes, MANET is susceptible to various attack, as well as routing protocol assumes that neighboring node is not malicious and all nodes will cooperate with each other to forward data for data communication. This assumption only, provides the attacker an opportunity to insert malicious or non cooperative nodes into the network.

In order to enhance the security level of MANET, it is desirable that MANET can detect attackers as soon as they enter or start its initial activity in the network, thus using Intrusion Detection System it would be possible to completely eliminate the damages caused by malicious node on to the data exchanged between nodes. MANET IDS can provide one layer of defense for MANETs.

To provide a high survivability for the system, IDS should complement existing prevention technique[27]. IDS monitors network traffic and node in a network as well as its behavior to detect malicious activity performed by suspicious node in network. There are various existing IDS in MANET to detect malicious behavior of node that can compromise the security of network.

II. METHODOLOGY

There are various intrusion detection system to detect malicious node in mobile adhoc network.

A. WATCHDOG

Marti et al[14] proposed a new IDS in MANET to improve throughput of network in presence of malfunctioning or misbehaving nodes named Watchdog. This technique consists of two parts, watchdog and pathrater, where watchdog is an IDS and pathrater is a result of IDS.

Watchdog is implemented in every node in the network and detects malicious node misbehavior in the network by overhearing of packets. It listens to its neighboring node and overhears that whether its next node forwards the packet. If the neighbor node fails to forward the packet it increases its failure counter. If the value of counter exceeds a predefined value which is set prior to transmission i.e. threshold then that particular node is reported as misbehaving by previous node. After the response of watchdog, a pathrater cooperates with routing protocol and avoids the misbehaving node to exist in the path of future transmission. Thus pathrater decides the routing path from source to destination such that the reported malicious node should not present in between. As compared to other technique watchdog detect malicious node rather than links. However the weakness of watchdog fails to detect malicious node in presence of ambiguous collision, receiver collision, limited transmission power, false misbehavior report and partial dropping.

1. **AMBIGUOUS COLLISION:** In ambiguous collision, collision prevents the node A from overhearing packet 1 from node B, because at the same time packet 2 was sent from source node. Thus node A comes in ambiguity and can't decide that collision occur by B or by some other neighbor of node A.

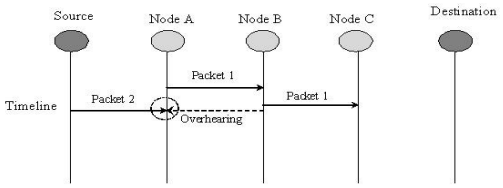

Fig.1: Ambiguous Collision

2. **RECEIVER COLLISION:** In this problem, Node A only overhears that node B has forwarded the packet 1 to node C and assumes that node C has received packet 1 but due to collision of packets at node C i.e. packet 2 from node N and packet 1 from node B ,Node C has dropped both packet and doesn't receive any packet.

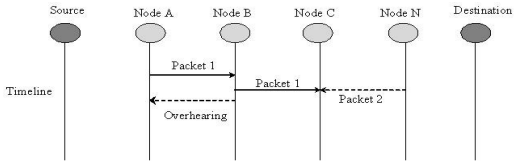

Fig.2 Receiver Collision

3. **LIMITED TRANSMISSION POWER:** Nodes in a MANET limit their transmission power to save battery resources. This leads to major drawback in watchdog. In this problem nodes B limits its transmission power by limiting its range. The misbehaving node limits its power such that it is strong enough to be overheard by previous node but is too weak to be received by destination node.

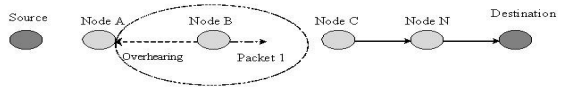

Fig.3 Limited Transmission Power

4. **FALSE MISBEHAVIOUR REPORT**: This problem occurs when a node falsely report other nodes as misbehaving. In this problem node A, acts as a suspicious node. In the path from source to destination, node A although overheard that node B has forwarded the packet to node C, node A still reported source node that node B is misbehaving by sending false misbehavior report.

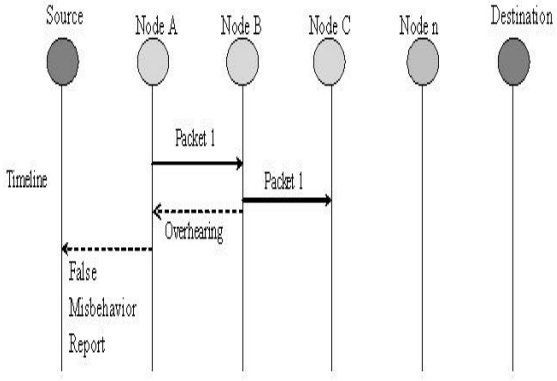

Fig 4: False Misbehavior Repor

B. TWOACK

TwoAck intrusion detection system is used to overcome the two major problems of watchdog i.e. receiver collision and limited transmission power. TwoAck detects malicious link rather than nodes. TwoAck scheme is named as because it works on 3 consecutive nodes i.e. 2 hops away from source node. In TwoAck scheme, node A sends packet n to node B, Node B forwards to node C, as node C is 2 hops away from source node, it is required to send back an TwoAck packet following the same route path from where the packet came but in reverse order. If source node receives TwoAck within time period it assures that packet transmission was successful otherwise the source node reports both nodes B and C as malicious. The drawback of this approach is that because of Ack packet transmission, it generates network overhead. Due to limited battery of node, this overhead reduces the life span of network.[13][16].

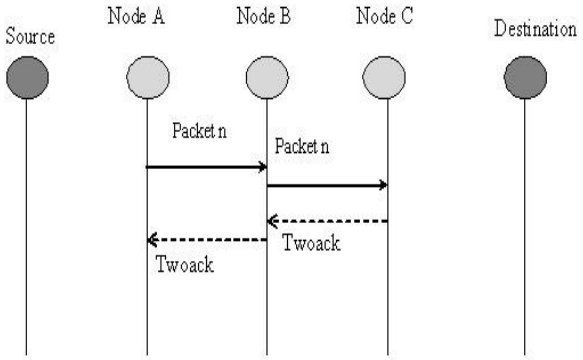

Fig.5 TwoAck Transmission

C. AACK

AACK (Adaptive Acknowledgment) is a network layer IDS based on acknowledgement. This is a combination of ACK and Tack (similar to TwoAck). The main advantage of ACK over TwoAck is that it reduce network overhead as compared to TwoAck as well as increases detection rate of malicious node [15]. It works on both schemes i.e. ACK and TACK. In this scheme, each node works in 2 nodes i.e. AACk node And TwoAck node. Depending on node, it sends data packet of one bit in the reserved field of DSR (i.e. AA data packet in case of AACK mode and TA data packet in case of TwoAck mode). According to mode, each node performs its work. By default each node is in AACK mode and each node sends AA data packet to destination node, after receiving destination node sends ACK in reverse route, if within time period the ACK

was received by source node then transmission was successful, otherwise source node switches its mode in TACK mode and sends TACK packet(TA) to destination mode. In this mode each node sends TwoAck packet to the previous 2 hop node to detect malicious node. However AACK scheme reduces overhead as compared toTwoAck but Still both scheme fails to detect malicious node in presence of false misbehavior report [12][16].

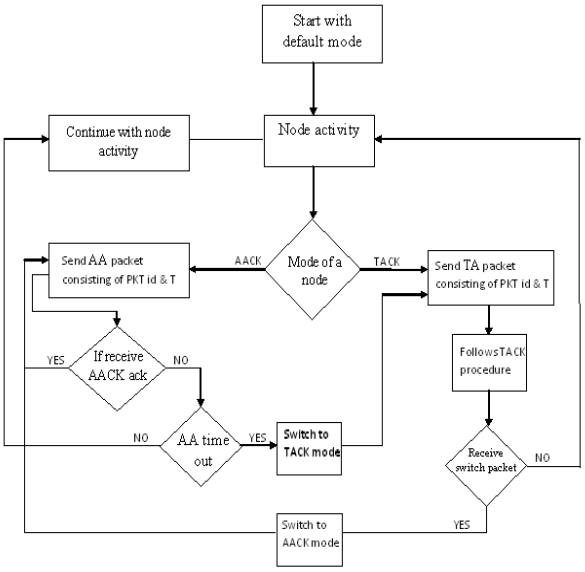

Fig.6 Flowchart of AACK

D. EAACK

EAACK is acknowledgement based IDS which is used to overcome the weakness of previously defined IDS. EAACK consist of three parts:

I. ACK
II. S-ACK
III. MRA

For identification of these packet, 2-b of the 6-b in the DSR header is used. However for further enhancement of this technique, in order to overcome the problem of forge acknowledgment [7] in addition with the weakness of watchdog, EAACK with digital signature is used. In this scheme, every ack packets are digitally signed by its sender and receiver.

I. **ACK**: Ack mode is the initial mode of EAACK scheme. It aims to reduce network overhead when no suspicious (misbehaving) node is detected. In this mode, source node sends data packet to destination node, and at the same time it stores the packet id and sending time. Destination node after receiving data packet it generates and sends Ack packet to source node on the reverse order of same route that consists of received packet id. If source node receives Ack packet within a predefined time period, data transmission from source to destination is successful, otherwise source node S will switch to S-ACK mode by sending S-Ack data packet (i.e. 2 b of 6 bit header of DSR) to destination node to detect malicious node in the network.

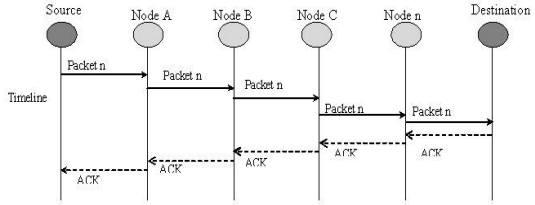

Fig.7 ACK Transmission

II. **S-ACK**: S-ACK is an enhancement of TwoAck scheme. The difference between both scheme is that in TwoAck source node trusts the received misbehavior report without confirming, however S-ACK switches to MRA mode for confirming this report. Similar to TwoAck, S-Ack works with three consecutive nodes together to detect suspicious node in the network, the only difference with respect to data packet is that in S-Ack mode, the data packet consists of flag to indicate the type of data packet. In this scheme, node A sends S-Ack data packet to node B which further forwards to node C. When node C receives data it sends S-Ack acknowledgment packet as it is 2 hops away from node A. If A receives S-Ack within predefined time period, the transmission is successful, otherwise both node B and C is reported as malicious and F1 generates the misbehavior report and send to source node. However source node does not immediately trust this misbehavior report and switch to MRA mode to confirm.

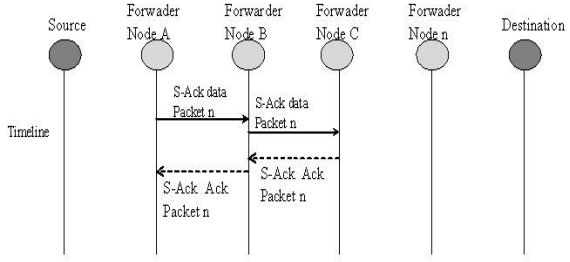

Fig. 8 S-ACK Transmission

III. **MRA**: MRA mode is basically used to detect malicious node in presence of false misbehavior report. This false misbehavior report is generated by malicious node in order to falsely show innocent node as malicious. The main aim of MRA node is to check whether the destination node has received the reported packet through different route to detect malicious node. Thus to start with MRA mode, the source node searches

a new route to destination firstly by searching its local database and seeking for a different route. If no different route exists in database it starts a DSR routing request to search for a different route. After searching and accepting the new route to destination it sends MRA packet (containing id of packet that has been sent out) to destination from a new route. When the destination node received an MRA packet, it searches its database and compares whether the received packet id was matched with the packet in the database. If there is a match, then it is verified that packet was already received and this a false misbehavior report and the node that generated this report is marked as malicious. If there is no match then this misbehavior report is marked as valid and is trusted and accepted.

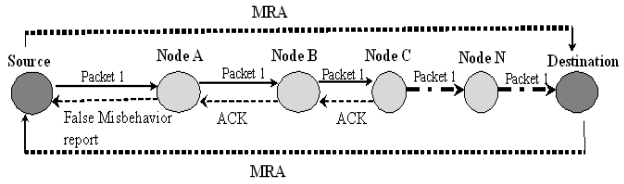

Fig.9. MRA packet Transmission

IV. **DIGITAL SIGNATURE**: As EAACK is an Ack based IDS all 3 parts of EAACK detect malicious node based on acknowledgment. However there is a need to secure ACK packet, otherwise all schemes of EAACK will be vulnerable. Thus to overcome the problem of forged acknowledgment there is a need to securely transfer ACK, EAACK uses DSA and RSA digital algorithm scheme. Therefore to ensure the integrity of IDS every packet before sending is digitally signed by the sender and is verified before they are accepted such that all Ack packets are authenticated and no sender can deny from sending.

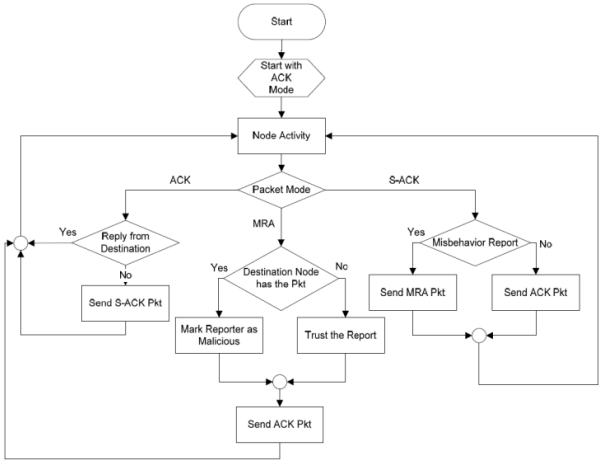

Fig. 10 Flowchart of EAACK

III. RESULT:

The result part will demonstrate the comparison between all methodologies i.e. DSR, Watchdog, TwoAck, AACK, EAACK in terms of Packet delievery ratio (PDR) , Routing Overhead and end to end delay.

The table 1 [12] will show the result of all methodology in terms of PDR. The table 2[12] will show result in terms of Routing overhead. The table 3 [16] will show result in terms of end to end delay.

TABLE 1

Malicious Node	PDR				
	DSR	*Watchdog*	*TwoAck*	*AACK*	*EAACK*
0	1	1	1	1	1
10	0.82	0.82	0.92	0.93	0.95
20	0.72	0.75	0.85	0.87	0.92
30	0.69	0.72	0.82	0.82	0.86
40	0.62	0.65	0.81	0.81	0.80

TABLE 2

Malicious Node	Routing Overhead				
	DSR	*Watchdog*	*TwoAck*	*AACK*	*EAACK*
0	0.03	0.03	0.19	0.19	0.19
10	0.03	0.03	0.22	0.22	0.22
20	0.03	0.03	0.38	0.25	0.31
30	0.03	0.03	0.41	0.27	0.29
40	0.03	0.03	0.51	0.51	0.51

TABLE 3

Malicious Node	End to End delay			
	DSR	*Watchdog*	*TwoAck*	*AACK*
0	0.031	0.031	0.055	0.065
10	0.015	0.015	0.051	0.059
20	0.012	0.012	0.049	0.051
30	0.011	0.011	0.042	0.042
40	0.011	0.011	0.033	0.032

V.CONCLUSION

From Table 1, Table 2 and Table 3 we can conclude that both DSR and Watchdog gives equal performance in terms of PDR and routing overhead and end to end delay. However due to its drawback TwoAck was used. But TwoAck suffered from greater routing overhead thus to reduce the network overhead AACK was used. AACK reduces routing overhead, but end to end delay was greater however if malicious node increases end to end delay and PDR of AACK was reduced. Thus AACK

was preferred as compared to TwoAck. As Security is prior, Eaack was introduced with digital signature in order to prevent attackers from forged acknowledgments. EAACK was very most preferable because of security. In EAACK for digital signature RSA and DSA is used however in RSA more malicious node generates more RO. In some cases it generates more PDR. However if malicious node increases PDR gets reduced. Furthermore PDR can be improved if attackers are smart enough to forge acknowledgment packets. In future end to end delay needs to calculated for EAACK as well as RO can reduced by using the most popular cryptography named Elliptic curve cryptography because of reduced key size.

REFERENCES:

[1] K. Al Agha, M.-H. Bertin, T. Dang, A. Guitton, P. Minet, T. Val, and J.-B. Viollet, "Which wireless technology for industrial wireless sensor networks? The development of OCARI technol," IEEE Trans. I nd. Elec- tron., vol. 56, no. 10, pp. 4266–4278, Oct. 2009.

[2] R. Akbani, T. Korkmaz, and G. V. S. Raju, "Mobile Ad hoc Net- work Security," in Lecture Notes in Electrical E ngineering , vol. 127. New York: Springer-Verlag, 2012, pp. 659–666.

[3] R. H. Akbani, S. Patel, and D. C. Jinwala, "DoS attacks in mobile ad hoc networks: A survey," in Proc. 2nd Int. Meeting ACCT , Rohtak, Haryana, India, 2012, pp. 535–541.

[4] T. Anantvalee and J. Wu, "A Survey on Intrusion Detection in Mobile Ad Hoc Networks," in Wireless/Mobile Security. New York: Springer-Verlag, 2008

[5] L. Buttyan and J. P. Hubaux, Security and Coopera tion in Wireless Networks. Cambridge, U.K.: Cambridge Univ. Press, Aug. 2007.

[6] D. Dondi, A. Bertacchini, D. Brunelli, L. Larcher, and L. Benini, "Model- ing and optimization of a solar energy harvester system for self-powered wireless sensor networks," IEEE Trans. I nd. Electron., vol. 55, no. 7, pp. 2759–2766, Jul. 2008.

[7] N. Kang, E. Shakshuki, and T. Sheltami, "Detecting forged acknowl- edgements in MANETs," in Proc. I EEE 25th I nt. C onf. AINA, Biopolis, Singapore, Mar. 22–25, 2011, pp. 488–494.

[8] Y. Hu, D. Johnson, and A. Perrig, "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks," in Proc. 4 th IEEE Wo rkshop Mobile Comput. S yst. Appl. , 2002, pp. 3–13.

[9] Y. Hu, A. Perrig, and D. Johnson, "ARIADNE: A secure on-demand rout- ing protocol for ad hoc networks," in Proc. 8 th AC M I nt. C onf. M obiCom, Atlanta, GA, 2002, pp. 12–23.

[10] G. Jayakumar and G. Gopinath, "Ad hoc mobile wireless networks rout- ing protocol—A review," J. Comput. S ci., vol. 3, no. 8, pp. 574–582, 2007.

[11] D. Johnson and D. Maltz, "Dynamic Source Routing in ad hoc wireless networks," in Mobile Computing . Norwell, MA: Kluwer, 1996, ch. 5, pp. 153–181.

[12] N. Kang, E. Shakshuki, and T. Sheltami, "Detecting misbehaving nodes in MANETs," in Proc. 12th I nt. C onf. iiWAS , Paris, France, Nov. 8–10, 2010, pp. 216–222.

[13] J.-S. Lee, "A Petri net design of command filters for semiautonomous mobile sensor networks," IEEE Trans. I nd. Electron., vol. 55, no. 4, pp. 1835–1841, Apr. 2008.

[14] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbe- haviour in mobile ad hoc networks," in Proc. 6 th Annu. Int. Conf. M obile Comput. N etw., Boston, MA, 2000, pp. 255–265.

[15] T. Sheltami, A. Al-Roubaiey, E. Shakshuki, and A. Mahmoud, "Video transmissionenhancementinpresenceofmisbehavingn odesinMANETs,"Int. J. Multimedia Syst. , vol. 15, no. 5, pp. 273–282, Oct. 2009.

[16] A Al-Roubaiey†, T. Sheltami†,‡, A. Mahmoud†, E. Shakshuki*, H. Mouftah," AACK: Adaptive Acknowledgment Intrusion Detection for MANET with Node Detection Enhancement",in AINA 2010 24th IEEE International Conference vol 634-640 April 2010.