# A SURVEY ON IDSS IN MANETS

[1]S. L. Kshirsagar, [2]A.R.Surve
Department of Computer Science & Engineering
Walchand college of Engineering, Sangli
Email: [1]slksagar@gmail.com, [2]Anil.surve@walchandsangli.ac.in

**Abstract— With the changing age of technology we are observing magnificent changes in the way of communication. We are speedily moving from the wired networks to the wireless networks, in the last decade there has been drastic increase in the use of wireless networks due to the great development of mobile technology and its efficiency to connect the world significantly. Mobile Adhoc Networks (MANETs) are playing crucial role in this transformation. They being infrastructure less networks are really useful in the mission critical applications like military and the areas where the natural calamities have occurred. In MANETS as each node can behave both as receiver and transmitter the formation of the network becomes very easy. regardless Of all the advantages MANETs are pretty vulnerable as per the security attacks are concerned ,as it is having free medium intruders can easily enter the medium and attack the system. Intrusion Detection Systems(IDS) are specifically designed to stop such kind of attacks on the system.these systems(IDS) find out the vulnerable nodes and prevent them from making the great damage to the systems Watchdog ,TWOACK, AACK,EAACK are some of the IDS used now a days. Further the use of hybrid cryptography has added extra security to it.**

**Keywords- MANETs, Intrusion Detection System, EAACK**

## 1. INTRODUCTION

MANETs are the collection of mobile nodes equipped with both transmitter and receiver and communicating over a bidirectional wireless link directly or indirectly. Depending on the communication range MANETs are divided into two types. If all the nodes in the network are in communication range and can communicate directly then they form Single-hop netwok [1]. While if for sending messages from one node to another node they have to go through the another nodes they form multi-hop network.

All the nodes in these networks rely on each other for transmission of data in the network. Introduction of some misbehaving nodes can bring the throughput of the network by substantial amount. Though MANETs are having self organized and self maintained network formed without any infrastructure it is having a great threat about the security measures [3]. Intrusion detection systems play vital role in removal of security threats. IDS monitors the behavior of different nodes and find out whether there is some node which is performing some malicious actions and causing problems for the networks. Some IDS work on basis of just monitoring the nodes while some work on the basis of responses like acknowledgements. As there is no physical protection to the network the intervention of intruders is quite easy in these types of networks because most protocols used in the MANETs assume every node in the network behaves cooperatively and not malicious. The sad thing about security is that many organizations in the world invest less in security issues than they are investing on the other common stuff as it is not providing any direct revenue due to this the security is too poor which further boosts the intruders.

## 2. IDS in MANETs

As discussed above due to the assumptions of routing protocols in MANETs that all the nodes behave co-operatively, MANETs become very easy to attack just by compromising one or two nodes. This is the reason IDS should be added to improve the level of security in the MANETs by removing the compromised nodes in the network. Some of them like Watchdog, AACK,TWOACK will be discussed in this paper.

### 2.1 Watchdog:

Watchdog is a scheme that is designed in way that it will improve the throughput of a network though there are malicious nodes in the network which are trying to bring down the performance [4]. Watchdog consist of two parts Watchdog and pathrater. Watchdog works as a IDS for MANETs. It continuously listens to the nodes in the network
and keeps eye on the malicious activities of the next nodes in the network. If it find out that the next node which is overheard is not transferring the packet to the subsequent ones then it increases the failure counter for that node. There is a predefined threshold defined for failure counter. If the failure counter crosses the threshold value tht node is declared as a malicious node by Watchdog. In this case the pathrater comes into act ,with the help of routing protocols it finds the new path for the transmission of packets so that the malicious node is avoided.

Studies have shown that Watchdog scheme is an efficient one[9][10][11]. What makes it more special is that it detcts the malicious nodes rather than the links. Watchdog has been appreciated and taken as a reference by many other IDS. The new system were developed either taking it as a base or improving the problems with it.

Though it is taken as a reference it is having certain problems [1] to figure out the malicious nodes in the following conditions . 1) Ambiguous collisions; 2) receiver collisions;
3) limited transmission power; 4) false misbehavior report;
5) Collusion; and 6) partial dropping.

### 2.2 TWOACK:

Many different researchers came out with their ideas to solve the problems with the Watchdog. TWOACK is one of the approach which was proposed by Liu et al[]. The difference between this method and others is that it is neither enhancement nor a scheme having its base as a watchdog. Watchdog finds out the malicious node but this system is more concerned about the links. It is an acknowledgement based scheme which works with the three consecutive nodes at a time. As soon as node receives a packet it has to send back acknowledgement to the node two hops down the route from it. TWOACK works with the dynamic source routing protocol.

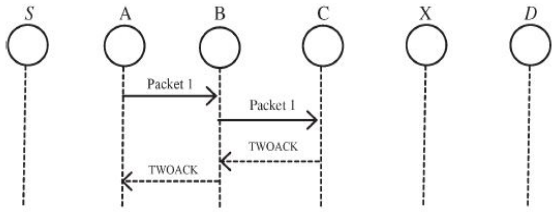



Fig1:TWOACK scheme

The figure shows how the TWOACK system works packet 1 is transmitted from A to B, B further pass it down to C. As soon as C receives the packet and it being two hop away from the source it sends back TWOACK packet down the line to A. The arrival of packet at A is indication that the packet has been transferred upto C successfully. If A doesnt get TWOACK packet in predefined time it reports both B and C as malicious nodes.

The TWOACK scheme solves the receiver collision and limited transmission power problems of Watchdog, but it creates excessive amount of acknowledgements which creates excessive overhead on network. It can create a lot of energy problems.

### 2.3 AACK:

This method which is based on the TWOACK method was proposed by Sheltami *et al* [4].This method is combination of two schemes TACK which is similar to TWOACK and ACK which is an end to end acknowledgement scheme. It substantially reduces the network traffic and perform as good as or sometimes better than the TWOACK.

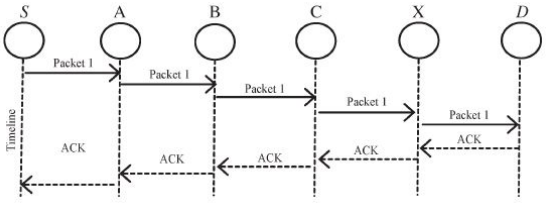



**Fig.2 ACK scheme.**

ACK scheme works as per shown in above figure 2. The source S has sent a packet for node D. The intermediate nodes just forward the packet to the next node. As soon as node D receives the packet it has to send back the packet to the node S in the reverse order of the same path. If S receives the packet in a predefined time period then transmission is successful otherwise S will move to the TACK mode. Using this hybrid technique we lower the network traffic by a great margin. Though this is the thing main problem with both TWOACK and AACK is that they suffer from the problem with the false misbehavior report and forced acknowledgements.

## 3. DIGITAL SIGNATURES

As we are using open medium in the MANETs security is a major concern for this. It is necessary to check whether the packets we have got are authentic or not. It will be secure if we communicate by using encrypted messages by using cryptographic methods. For integrity, authentication and nonrepudiation we use Digital Signatures. We use public key cryptography and hashing for creating Digital Signatures.

## 4. EAACK

EAACK is IDS for MANETs which is designed to solve three out of six problems in the Watchdog receiver collision, limited transmission power and false misbehavior report.

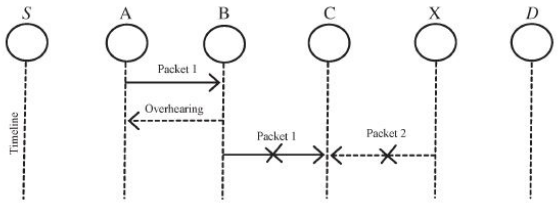



**Fig3.Receiver collision**

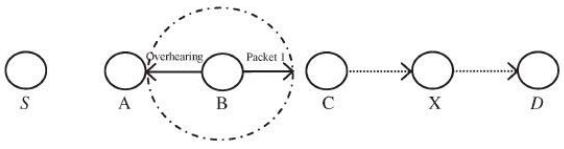



**Fig.4. Limited Transmission Power**

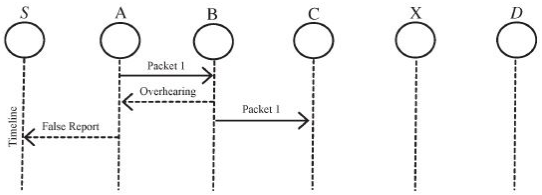



**Fig.5 False Misbehavior report**

The above three diagrams show the three problem with the watchdog

### 4.1 Receiver collision:

fig.3 shows what exactly the receiver collision problem is. Node A sends the packet to node B. It further overhears whether B has forwarded the packet to C. At the same time node X is also sending packet to C. In such a case A overheard that packet has been successfully forwarded by B, but it fails to detect that node C has failed to receive the packet due to collision at C.

### 4.2 Limited Transmission Power:

In this case a node behaves selfishly; it limits its transmission power so that it can be overheard by only certain nodes. As shown in fig. 4 node B limits its transmission power so it can be overheard by A but not by the node C.

### 4.3False Misbehavior Report:

In false misbehavior report node A has sent packet 1 to B which B has forwarded successfully to C still A has reported B as misbehaving node as shown in fig. 5.

TWOACK and AACK can solve the first two of these three problems but fail for the third one. EAACK solves the three problems more promisingly.

EAACK is consisting of 3 major phases ACK, Secure ACK(S-ACK) and misbehavior report authentication (MRA).The packets are distinguished using two bits packet header included in EAACK.

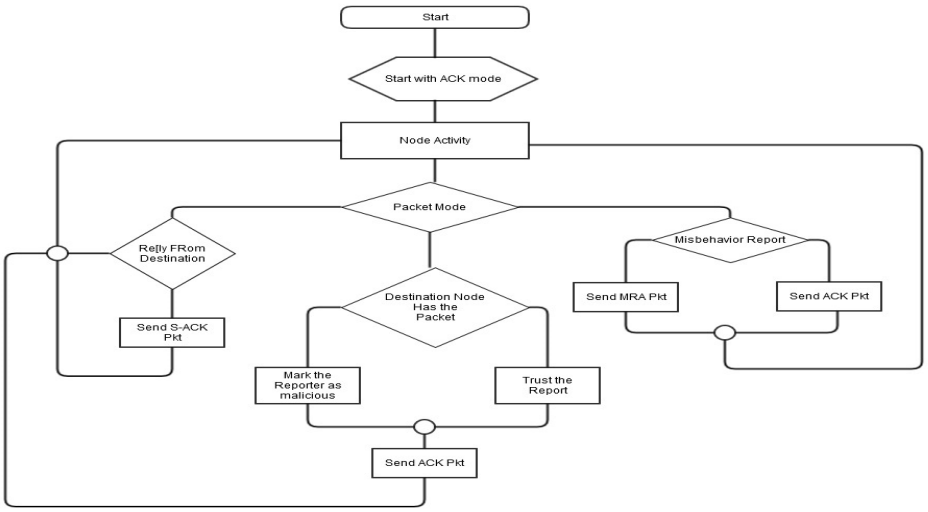
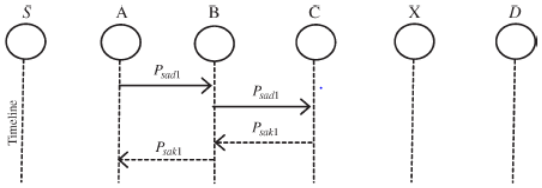



**Fig.6 EAACK scheme**

Fig.6 EAACK scheme
Above figure illustrates the working of the EAACK scheme. It goes through the three different phases before reporting a node as a malicious.

**4.4 ACK:**
ACK in general is an end to end acknowledgement scheme, here it works as a part of hybrid scheme to minimize the network overhead when everything is working fine. In this case the source sends a packet to destination if all the intermediate nodes cooperate then the packet will be forwarded to the destination. Destination has to send back the acknowledgement to the source in a predefined time so it is assumed to be successful. Otherwise the source has to switch to the S-ACK mode.

**4.5 S-ACK**:
After the node fails to receive an acknowledgement it switches to the A-ACK mode which is improved version of TWOACK scheme .The group of three consecutive nodes is taken in consideration to find out misbehaving nodes.




Node A has sent the S-ACK data sad1 to B which it has transferred to C as the node C is two hops away from the source it has to send back S-ACK acknowledgement packet back to the A on the same path. If acknowledgement is not sent back to A, it will send misbehavior report to the source S.
At this time source will move to MRA mode.

**4.6 MRA** :
This is vital step in the EAACK scheme to detect false misbehavior of the nodes. Some nodes may send false misbehavior report which will be indicating the nodes as a malicious nodes falsely.

In this mode the source node checks its local database to check whether there is another path for that destination node. If there is no such path existing then it will start DSR routing request. By doing this we will reach the destination by another path. After receiving the packet receiver will check its l
destination the misbehavior report is wrong otherwise it has to be trusted.

**4.7 Digital Signature:**
All the three parts are acknowledgement based schemes. They all believe on Acknowledgements to detect the malicious nodes in the network so it is so much important

to check the authenticity of the packets. Digital signatures provide the required authentication in this scheme. DSA and RSA are used for this.

## 5. PERFORMANCE METRICS

The performance of the different IDS can be measured on the basis of the following metrics.

### 5.1 Packet delivery ratio (PDR*)*:

PDR defines the ratio of the number of packets received by the destination node to the number of packets sent by the source node

**5.2 Routing overhead (RO)**: RO defines the ratio of the amount of routing-related transmissions [Route REQuest(RREQ), Route REPly (RREP), Route ERRor (RERR), ACK, S-ACK, and MRA].

We can check performance of the systems in different scenarios like packet dropping and false misbehavior.

## 6. CONCLUSION

Security has become a great concern in MANETs

And we are coming across different types of IDS day by day. In the studies we found that WATCHDOG has been reference for most of these systems. It has been surrounded by lot of problems. TWOACK and AACK solve some of the problems but suffer from some problems like network overhead and false misbehavior report. EAACK has evolved as one of the best IDS which outperforms the other schemes substantially.

EAACK further adds the security to the communication and doing so helps to improve the faith in the users to use the network. The hybrid technologies are evolving as a reat source for the security.

## 7. REFFERENCES

[1]EAACK – A Secure Intrusion Detection System for MANETs Elhadi M. Shakshuki, Senior Member, IEEE, Nan Kang and Tarek R. Sheltami, Member, IEEE

[2]K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An acknowledgment-based approach for the detection of routing misbehaviour in MANETs," *IEEE Trans. Mobile Comput.*, vol. 6, no. 5 pp. 536–550

[3] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehaviour in mobile adhhoc networks," in *Proc. 6th Annu. Int. Conf. Mobile Comput. Netw.*, Boston, MA, 2000, pp. 255–265

[4] T. Sheltami, A. Al-Roubaiey, E. Shakshuki, and A. Mahmoud, "Video transmission enhancement in presence of misbehaving nodes inMANETs," *Int. J. Multimedia Syst.*, vol. 15 no. 5, pp. 273–282, Oct. 2009.

[5] V. C. Gungor and G. P. Hancke, "Industrial wireless sensor networks:
Challenges, design principles, and technical approach," *IEEE Trans. Ind. Electron.*, vol. 56, no. 10, pp. 4258–4265, Oct. 2009.

[6] Y. Hu, D. Johnson, and A. Perrig, "SEAD: Secure efficient distance vector
routing for mobile wireless ad hoc networks," in *Proc. 4th IEEEWorkshop Mobile Comput. Syst. Appl.*, 2002, pp. 3–13.

[7] Y. Hu, A. Perrig, and D. Johnson, "ARIADNE: A secure on-demand routing protocol for ad hoc networks," in *Proc. 8th ACM Int. Conf. MobiCom*,Atlanta, GA, 2002, pp. 12–23.

[8] G. Jayakumar and G. Gopinath, "*Ad hoc* mobile wireless networks routing protocol—A review," *J. Comput. Sci.*, vol. 3, no. 8, pp. 574–582,2007.

[9] 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.

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