Volume-6,Issue-1 (Aug-16)
ISSN (O) :- 2349-3585

Improved EAACK Intrusion Detection System for MANET - A Study

Randeep Kaur Kahlon[1], Dr.J.W.Bakal[2]
[1]Assistant Professor, [2]Principal,
[1]Dt. of Computer Technology,
[1]Terna College Of Engineering, Navi Mumbai, Maharashtra, India.
[2]Jondhale College Of Engineering, Dombivli, Maharashtra, India.

***Abstract*- The journey to wireless network from wired network has been adopted in the past few decades. MANET, mobile ad-hoc network is one of the most vital applications of wireless network. Due to the self configuring ability of nodes and its infrastructure less nature, MANET is preferred in significant applications. MANET is used in military and natural disasters applications. Security measures play an important role in all these applications. In MANET, all the nodes are assumed to be co-operative. If an individual mobile node attempt to benefit from other nodes, but refuse to share its own resources. Such nodes are called misbehaving nodes and their behavior is termed as misbehavior. Hence it is necessary to develop intrusion-detection system for MANET to identify malicious nodes in the network. Many IDS have been proposed for detecting malicious nodes. In this paper, we study various IDS proposed by researchers and do comparative study.**

INTRODUCTION

MANET

MANET (Mobile Ad hoc network) is a collection of mobile nodes equipped with both a wireless transmitter and receiver communicating via each other using bidirectional wireless links directly or indirectly. The nodes in the network function as routers, clients, and servers. The 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. In a single-hop network, all nodes within the same radio range communicate directly with each other. In a multihop network, nodes rely on other intermediate nodes to transmit if the destination node is out of their radio range. MANETs lack central administration and prior organization, so the security concerns are different than those that exist in conventional networks.

MANET is more vulnerable than wired network. Some of the vulnerabilities are as follows:-

- Lack of centralized infrastructure.
- Resource availability.
- Scalability.
- Cooperativeness.
- Limited power supply.
- Bandwidth restriction.
- Adversary inside the Network.
- No predefined Boundary.

Wireless links makes MANET more susceptible to attacks. It is easier for hackers to eavesdrop and gain access to confidential information. It is also easier for them to enter or leave a wireless network because no physical connection is required. They can also directly attack the network to delete messages, inject false packets, or impersonate a node. This violates the networks goals of availability, integrity, authentication, and no repudiation. Compromised nodes can also launch attacks from within a network. Most routing protocols in MANETs assume that every node in the network behaves cooperatively with other nodes and presumably not malicious, attackers can easily compromise MANETs by inserting malicious or non cooperative nodes into the network. An individual mobile node may attempt to benefit from other nodes, but refuse to share its own resources. Such nodes are

called misbehaving nodes and their behavior is termed misbehavior. In such case, it is crucial to develop an intrusion-detection system (IDS) specially designed for MANETs.

IDS

Intrusion means any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource. Intrusion Prevention is the primary security because the primary step is to make the systems safe from attacks by using passwords, biometrics etc. Even if intrusion prevention methods are used, the system may be subjected to some vulnerability. So we need a Intrusion Detection Systems (IDSs), to detect and produce responses if necessary. An IDS collects activity information and then analyzes it to determine whether there are any activities that violate the security rules.

In this paper, we classify the IDS in MANET. Current intrusion detection systems corresponding to those architectures are reviewed and compared. The rest of the paper is structured as follows. Section 2 describes the background on intrusion detection systems. In Section 3, schemes that have been introduced for IDS in MANETs are presented.

Some of the intrusion detection techniques are reviewed and compared in Section 4. Finally, the conclusion is given in Section 5.

RELATED WORK

Marti, Giuli, Lai and Baker[1] described the two techniques that increase the throughput in the presence of nodes that agree to forward the packets but fail to do so. The techniques are Watchdog and Pathrater. In watchdog, suppose S send data to D, then all the intermediate nodes stores packets in the buffer. If the packet remains with the node more than the timeout value then failure tally is incremented by Watchdog. Then if the failure tally increases than the threshold value then Watchdog detects node as malicious node and sends message to the source. Watchdog increases the throughput of network to 27% but increases the network overhead to 24% from 17%. Watchdog identifies the misbehaving nodes and Pathrater avoids the routing through these nodes. 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.

To overcome the weakness of Watchdog and Pathrater, Nasser and Chen introduced intrusion detection system called ExWatchdog[2]. Through overhearing, each node can detect the malicious action of its neighbors and report other nodes. However, if the node that is overhearing and reporting itself is malicious, then it can cause serious impact on network performance. The main concern here was to discover malicious nodes which can partition the network by falsely reporting other nodes as misbehaving and then proceeds to protect the network. Routeguard assigns ratings to nodes and calculates a path metric in a refined way. If the real malicious node is on all paths from specific source and destination, then it is impossible for the source node to confirm with the destination of the correctness of the report. It decreases network overhead. Parker[3] presents network intrusion detection mechanisms that uses snooping algorithm to detect misbehavior in the mobile adhoc networks. Two response mechanisms are used - Passive to detect if node is intrusive and protects itself from attacks and Active to detect if node is intrusive and act to protect all nodes from attacks. A mis-route cannot be determined but any modification and packet dropping can be identified and locked. TWOACK proposed by Liu et al. [4] is neither an enhancement nor a Watchdog-based scheme. TWOACK detects misbehaving links by acknowledging every data packet trans-mitted over every three consecutive nodes along the path from the source to the destination. Upon retrieval of a packet, each node along the route is required to send back an acknowledgment packet to the node that is two hops away from it down the route. TWOACK is required to work on routing protocols such as Dynamic Source Routing (DSR). Node A first forwards Packet 1 to node B, and then, node B forwards Packet 1 to node C. When node C receives Packet 1, as it is two hops away from node A, node C is obliged to generate a TWOACK packet, which contains reverse route from node A to node C, and sends it back to node A. The retrieval of this TWOACK packet at node A indicates that the transmission of Packet 1 from node A to node C is successful. Otherwise, if this TWOACK packet is not received in a predefined time period, both nodes B and C are reported malicious. The TWOACK scheme successfully solves the receiver collision and limited

ISSN:-2349-3585 |www.ijrdt.org

transmission power problems posed by Watchdog. The acknowledgment process required in every packet transmission process added a significant amount of unwanted network overhead. Based on TWOACK, Sheltami et al. [5] proposed a new scheme called AACK. Similar to TWOACK, AACK is an acknowledgment-based network layer scheme which can be considered as a combination of a scheme called TACK (identical to TWOACK) and an end-to-end acknowledgment scheme called ACKnowledge (ACK). Within a predefined time period, if the source node S receives this ACK acknowledgment packet, then the packet transmission from node S to node D is successful. Otherwise, the source node S will switch to TACK scheme by sending out a TACK packet. They fail to detect malicious nodes with the presence of false misbehaviour report and forged acknowledgment packets.To remove maximum problem of watchdog which cannot be solved by previous methods the new Enhanced AACK (EAACK) scheme[6] is developed and evaluated through implementation. It solves four significant problems of Watchdog mechanism, which are ambiguous collisions, receiver collisions, limited transmission power and false misbehavior report. It detects the malicious nodes by verifying ACK packets. Security is not provided over here for ACK packets. Hence, there is possibility that ACK packet is misused or not send from intended receiver. EAACK suffers from the threat that it fails to detect misbehaving node when the attackers are smart enough to forge the acknowledgement packets. Hence, Sheltami[7] introduced Digital Signature Algorithm (DSA) into the EAACK scheme, and investigate the performance of DSA in MANET. The purpose of this paper is to present an improved version of EAACK called EAACK2 that performs better in the presence of false misbehavior and partial dropping.Sheltami[8] introduced Digital Signature Algorithm (DSA) and RSA both into the EAACK scheme, and investigated the performance of DSA as well as RSA in MANET. They arrived to the conclusion that the DSA scheme is more suitable to be implemented in MANETs. It reduces network overhead. The threats an ad hoc network faces and the security goals to be achieved must be considered. It should focus on how to secure routing and how to establish a secure key management in an ad hoc networking environment. To build a highly available and highly secure key management service, threshold cryptography [9] has been proposed to distribute trust among a set of servers. AODV is also considered in detail and developed a security mechanism to protect its routing information [10]. The Secure Efficient Ad hoc Distance vector routing protocol (SEAD)[11], a secure ad hoc network routing protocol based on the design of the Destination-Sequenced Distance-Vector routing protocol. In order to support use with nodes of limited CPU processing capability, and to guard against Denial of- Service attacks in which an attacker attempts to cause other nodes to consume excess network bandwidth or processing time, it used efficient one-way hash functions and do not use asymmetric cryptographic operations in the protocol. Bandwidth and power constraints are the important factors to be considered in current wireless network because multi-hop ad-hoc wireless relies on each node in the network to act as a router and packet forwarder [12]. This dependency places bandwidth, power computation demands on mobile host to be taken into account while choosing the protocol.

IDS FOR MANET

In this section, we will study all proposed IDS schemes in detail.

WATCHDOG

Marti et al. [1] proposed a scheme named Watchdog that aims to improve the throughput of network with the presence of malicious nodes. Suppose there exists a path from node S to D through intermediate nodes A, B and C. Thus, when A transmits a packet for B to forward to C, A can often tell if B transmits the packet. Figure 1 illustrates how the watchdog works. When B forwards a packet from S towards D through C, A can overhear Bs transmission and can verify that B has attempted to pass the packet to C. The solid line represents the intended direction of the packet sent by B to C, while the dashed line indicates that A is within transmission range of B and can overhear the packet transfer.

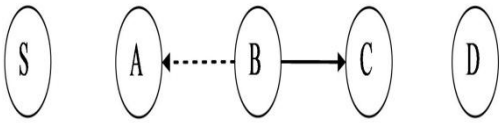

Fig. 1. Working of watchdog.

The watchdog is implemented by maintaining a buffer of recently sent packets and comparing each overheard packet with the packet in the buffer to see if there is a match. If so, the packet in the buffer is removed and forgotten by the watchdog, since it has been forwarded on. If a packet has remained in the buffer for longer than a certain timeout, the watchdog increments a failure tally for the node responsible for forwarding on the packet. If the tally exceeds a certain threshold bandwidth, it determines that the node is misbehaving and sends a message to the source notifying it of the misbehaving node. The Watchdog scheme is consisted of two parts, namely, Watchdog and Pathrater. Watchdog detects malicious misbehaviours by listening to its next hops transmission. The Pathrater cooperates with

the routing protocols to avoid the reported nodes in future transmission. The Pathrater assigns rating to nodes. When calculating path rates, if all other nodes are neutral nodes (rather than suspected misbehaving nodes), the Pathrater picks the shortest length path. Advantages :- Many research studies and implementations have proved that the Watchdog scheme is e client. These advantages have made the Watchdog scheme a popular choice in the field. Disadvantages:- The Watchdog scheme fails to detect malicious misbehaviours with the presence of :ambiguous collisions; receiver collisions; limited transmission power; false misbehaviour report; collusion; and partial dropping.

Let us see one by one problem,

AMBIGUOUS COLLISIONS

The ambiguous collision problem prevents A from overhearing transmission from B. As Figure 2 illustrates, Node A does not hear B forward packet 1 to C, because Bs trans-mission collides at A with packet 2 from the source

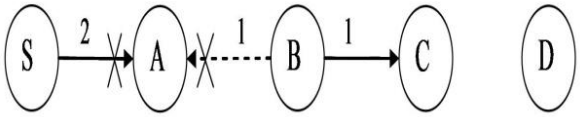

Fig. 2 Ambiguous Collision

A packet collision can occur at A while it is listening for B to forward on a packet. A does not know if the collision was caused by B forwarding on a packet as it should or if B never forwarded the packet and the collision was caused by other nodes in As neighborhood. Because of this uncertainty, A should not immediately accuse B of misbehaving, but should instead continue to watch B over a period of time. If A repeatedly fails to detect B forwarding on packets, then A can assume that B is misbehaving.

RECEIVERS COLLISION

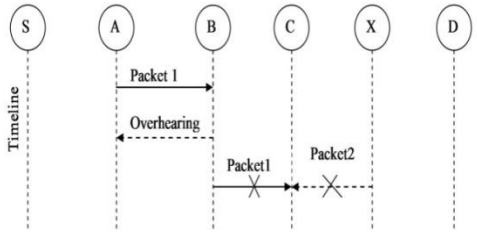

Fig. 3 Receiver collisions.

In receiver collisions, shown in Figure 3, Node A believes that B has forwarded packet 1 on to C, through C never received the packet due to a collision with packet 2 and 2.4 Both nodes B and X are trying to send Packet 1 and Packet 2, respectively, to node C at the same time. After node A sends Packet 1 to node B, it tries to overhear if node B forwarded this packet to node C; meanwhile, node X is forwarding Packet 2 to node C. In such case, node A overhears that node B has successfully forwarded Packet 1 to node C but failed to detect that node C did not receive this packet due to a collision between Packet 1 and Packet 2 at node C.

LIMITED TRANSMISSION POWER

In the case of limited transmission power, in order to preserve its own battery resources, node B intentionally limits its transmission power so that it is strong enough to be over-heard by node A but not strong enough to be received by node C, as shown in Figure 4.

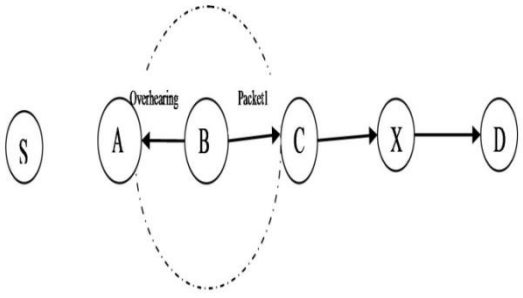

Fig. 4. Limited transmission power.

FALSE MISBEHAVIOUR REPORT

For false misbehaviour report, although node A successfully overheard that node B for-warded Packet 1 to node C, node A

still reported node B as misbehaving, as shown in Fig. 5.Due to the open medium and remote distribution of typical MANETs, attackers can easily capture and compromise one or two nodes to achieve this false misbehavior report attack.

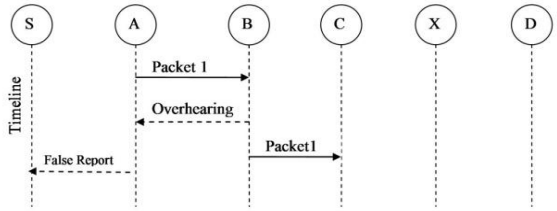

Fig. 5. False misbehaviour report.

COLLUSION

Multiple nodes in collusion can mount a more sophisticated attack. For example, B and C from Figure 2 could collude to cause mischief. In this case, B forwards a packet to C but does not report to A when C drops the packet. Because of this limitation, it may be necessary to disallow two consecutive untrusted nodes in a routing path.

PARTIAL DROPPING

A node can circumvent the watchdog by dropping packets at a lower rate than the watch-dog configured minimum misbehaviour threshold. With respect to the six weaknesses of the Watchdog scheme, many researchers proposed new approaches to solve these issues.

TWOACK

TWOACK proposed by Liu et al. [4] is neither an enhancement nor a Watchdog-based scheme. TWOACK detects misbehaving links by acknowledging every data packet trans-mitted over every three consecutive nodes along the path from the source to the destination. Upon retrieval of a packet, each node along the route is required to send back an acknowledgment packet to the node that is two hops away from it down the route.

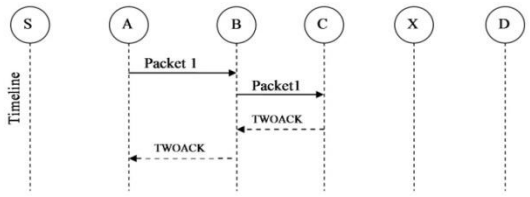

Fig.6. TWOACK scheme.

The working process of TWOACK is shown in Figure 6. Each node is required to send back an acknowledgment packet to the node that is two hops away from it. Node A rst forwards Packet 1 to node B, and then, node B forwards Packet 1 to node C. When node C receives Packet 1, as it is two hops away from node A, node C is obliged to generate a TWOACK packet, which contains reverse route from node A to node C, and sends it back to node A. The retrieval of this TWOACK packet at node A indicates that the transmission of Packet 1 from node A to node C is successful. Otherwise, if this TWOACK packet is not received in a predefined time period, both nodes B and C are reported malicious.

The same process applies to every three consecutive nodes along the rest of the route.

Advantages:- The TWOACK scheme successfully solves the receiver collision and limited transmission power problems posed by Watchdog.

Disadvantages:- The acknowledgment process required in every packet transmission process added a significant amount of unwanted network overhead.

AACK

Based on TWOACK, Sheltami et al. [5] proposed a new scheme called AACK. Similar to TWOACK, AACK is an acknowledgment-based network layer scheme which can be considered as a combination of a scheme called TACK (identical to TWOACK) and an end-to-end acknowledgment scheme called ACKnowledge (ACK).

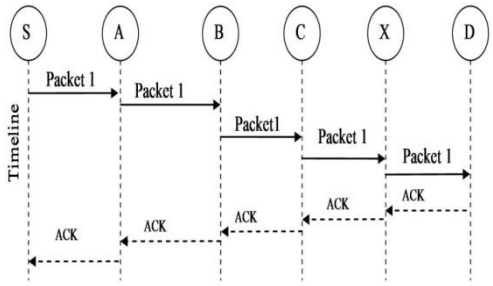

Fig.7 ACK Scheme

In the ACK scheme shown in Figure7, the destination node is required to send back an acknowledgment packet to the source node when it receives a new packet, the source node S sends out Packet 1 without any overhead except 2 b of ag indicating the packet type. All the intermediate nodes simply forward this packet. When the destination node D receives Packet 1, it is required to send back an ACK acknowledgment packet to the source node S along the reverse order of the same route.

ISSN:-2349-3585 |www.ijrdt.org

Within a predefined time period, if the source node S receives this ACK acknowledgment packet, then the packet transmission from node S to node D is successful. Otherwise, the source node S will switch to TACK scheme by sending out a TACK packet.

Advantages:- Compared to TWOACK, AACK significantly reduced network overhead while still capable of maintaining or even surpassing the same network throughput.

Disadvantages:- The concept of adopting a hybrid scheme in AACK greatly reduces the network overhead, but both TWOACK and AACK still suffer from the problem that they fail to detect malicious nodes with the presence of false misbehavior report and forged acknowledgment packets.

EAACK

To remove maximum problem of watchdog which cannot be solved by previous methods the new Enhanced AACK (EAACK) scheme is developed and evaluated through implementation [6]. EAACK was designed to tackle four of the six weaknesses of Watchdog scheme, namely, ambiguous collisions, false misbehavior, limited transmission power, and receiver collision. EAACK is consisted of three major parts, namely, ACK, secure ACK (S-ACK), and misbehavior report authentication (MRA). In order to distinguish different packet types in different schemes, they included a 2-b packet header in EAACK. There is 6 b reserved in the DSR header. In EAACK, they used 2 b of the 6 b to ag different types of packets. Details are listed in Table I.

TABLE I

Packet Type Indicator EAACK	
Packet Type	**Packet Flag**
General Data	00
ACK	01
S-ACK	10
MRA	11

Figure 8 presents a flowchart describing the EAACK scheme. In this scheme, they assumed that the link between each node in the network is bidirectional. Furthermore, for each ambiguous collision, receiver collision or limited transmission power. As shown in Figure 9, Node C is required to send back an acknowledgment packet to node A. In S-ACK mode, the three consecutive nodes (i.e., A, B, and C) work in a group to communication process, both the source node and the destination node are not malicious.

ACK

As discussed before, 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. Just like shown in Figure 7, in ACK mode, node S first sends out an ACK data packet Pad1 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 Pad1, node D is required to send back an ACK acknowledgment packet Pak1 along the same route but in a reverse order. Within a predefined time period, if node S receives Pak1, 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.

S-ACK

The S-ACK scheme is an improved version of the TWOACK scheme proposed by Liu et al. [4]. 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 was to detect misbehaving nodes in the presence of

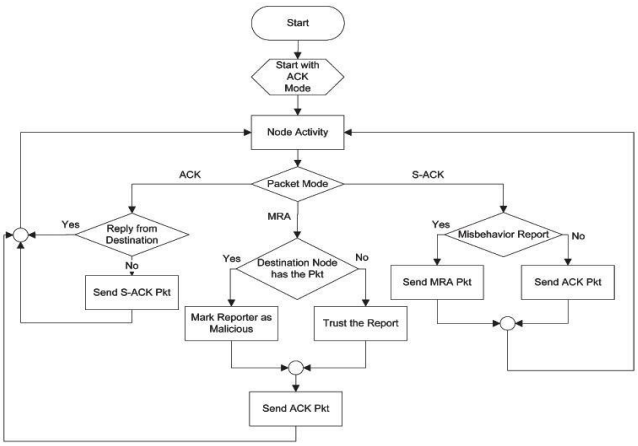

Fig 8. System control flow of EAACK scheme.

detect misbehaving nodes in the network. Node A first sends out S-ACK data packet Psad1 to node B. Then, node B forwards this packet to node C. When node C receives Psad1, as it is the third node in this three-node group, node C is

required to send back an S-ACK acknowledgment packet Psak1 to node B. Node B forwards Psak1 back to node A.

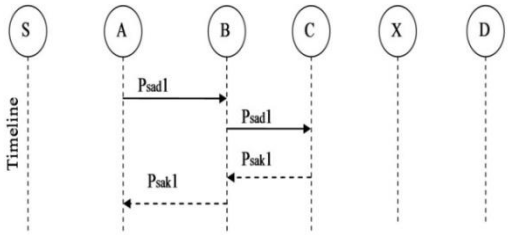

Fig.9. S-ACK scheme.

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 A 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.

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 fatal 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 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 send another route. Due to the nature of MANETs, it is common to find out multiple routes between two nodes. 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. By the adoption of MRA scheme, EAACK is capable of detecting malicious nodes despite the existence of false misbehavior report.

DIGITAL SIGNATURE

It is extremely important to ensure that all acknowledgment packets in EAACK are authentic and untainted. Otherwise, if the attackers are smart enough to forge acknowledgment packets, all of the three schemes will be vulnerable.

With regard to this urgent concern, digital signature ensure the integrity of the IDS, EAACK requires all acknowledgment packets to be digitally signed before they are sent out and verified until they are accepted is incorporated in EAACK scheme[7]. In order to ensure the integrity of the IDS, EAACK requires all acknowledgment packets to be digitally signed before they are sent out and verified until they are accepted.

COMPARATIVE STUDY

We will consider each of the above IDS, and give their advantages and disadvantages in Table 2 . The performance of all these schemes is compared by using parameters routing overhead and packet delivery ratio by using Ns2 simulator[9].

IDS Schemes	Advantages	Disadvantages
Watchdog and Pathrater	Throughput is increased by 27%. It analyses the effects of routing misbehavior in adhoc networks.	Routing Overhead is increased from 9% to 17%. It fails in various conditions: 1) ambiguous collisions; 2) receiver collisions; 3) limited transmission power; 4) false misbehavior report; 5) collusion; and 6) partial dropping.
Ex-Watchdog and Routeguard	Discovers malicious nodes which can partition the network by falsely reporting other nodes as misbehaving and then proceeds to protect the network. Reduces network overhead.	If the real malicious node is on all paths from specific source and destination, then it is impossible for the source node to confirm with the destination the correctness of the report.
TWOACK	Overcomes two drawbacks of Watchdog : receiver collisions and limited transmission power. Detect routing misbehavior and mitigate their adverse effect by using three nodes.	Adds unwanted network overhead. Not works in case of false misbehaviour report.
AACK	Overcomes the unwanted routing overhead caused by TWOACK. Detects misbehaving links by acknowledging every data packet trans-mitted over every three consecutive nodes along the path from the source to the destination.	They fail to detect malicious nodes with the presence of false misbehaviour report and forged acknowledgment packets.
EAACK	Solves four significant problems of Watchdog mechanism, which are ambiguous collisions, receiver collisions, limited transmission power and false misbehavior report.	It fails to detect misbehaving node when the attackers are smart enough to forge the acknowledgement packets. Reduces network overhead.
EAACK with DSA	Overcomes the problem of Forged Acknowledgements. Security is provided by using digital signatures. Performs better in the presence of false misbehavior and partial dropping.	Network routing overhead increases when number of malicious nodes increases.
EAACK with DSA and RSA	DSA scheme is more suitable to be implemented in MANETs. It reduces network overhead.	Encryption to data packets is not provided. Network routing overhead increases when number of malicious nodes increases.

ISSN:-2349-3585 |www.ijrdt.org

With regard to this urgent concern, digital signature ensure the integrity of the IDS, EAACK requires all acknowledgment packets to be digitally signed before they are sent out and verified until they are accepted is incorporated in EAACK scheme[7]. In order to ensure the integrity of the IDS, EAACK requires all acknowledgment packets to be digitally signed before they are sent out and verified until they are accepted.

COMPARATIVE STUDY

We will consider each of the above IDS, and give their advantages and disadvantages in Table 2 . The performance of all these schemes is compared by using parameters routing overhead and packet delivery ratio by using Ns2 simulator[9].

CONCLUSION

Attacks has always been a major threat to the security in wireless networks. In our paper, we have studied all the Intrusion Detection Systems. All the IDS were implemented and results are shown. The security has been implemented in the Acknowledgement packets. The acknowledgement packets are digitally signed and sent from source to destination. The EAACK scheme is implemented by using both RSA and DSA algorithms. The acknowledgement packets are of three types: ACK, S-ACK and MRA. The EAACK scheme solves all the drawbacks of the previous schemes. It identifies the malicious nodes as well as any forged acknowledgements present in the network. The routing overhead is also reduced than methods used in previous schemes. There are some limitations of EAACK scheme. It does not encrypts the data packets. The network routing overhead increases as number of malicious nodes increase in the network. We propose new scheme which incorporates hybrid cryptography and will compare it against existing mechanism in different scenarios through simulations. The hybrid cryptography concept improves security. It improves the network's PDR when the attackers are smart enough to forge acknowledgment packets. Hybrid Cryptography like Triple DES, MD5 and RSA algorithm can improve confidentiality, availability and integrity of the system. So our proposed system can ensure more security to the network and also improve throughput.

REFERENCES

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

[2] J. Parker, J. Undercoffer, J. Pinkston, and A. Joshi, "On intrusion detection and response for mobile ad hoc networks," in Proc. IEEE Int. Conf.Perform., Comput., Commun., 2004, pp. 747–752.

[3] N. Nasser and Y. Chen, "Enhanced intrusion detection systems for discovering malicious nodes in mobile ad hoc network," in Proc. IEEE Int. Conf. Commun., Glasgow, Scotland, Jun. 24–28, 2007, pp. 1154–1159

[4] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, ―An Acknowledgment-based Approach for the Detection of Routing Misbehavior in MANETs‖, IEEE Transactions on Mobile Computing, May 2007.

[5] Al-Roubaiey, A.; Sheltami, T.; Mahmoud, A.; Shakshuki, E.; Mouftah, H., "AACK: Adaptive Acknowledgment Intrusion Detection for MANET with Node Detection Enhancement," Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference on , vol., no., pp.634-640, 20-23April2010.

[6] 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.

[7] N. Kang, E. Shakshuki, and T. Sheltami, "Detecting forged acknowledgements in MANETs," in Proc. IEEE 25th Int. Conf. AINA, Biopolis,Singapore, Mar. 22–25, 2011, pp. 488–494.

[8] Elhadi M. Shakshuki, Nan Kang, and Tarek R. Sheltami ― EAACK—A Secure Intrusion-Detection System for MANETs, IEEE Transactions on Industrial Electronics, Vol. 60, No 3, March 2013.

[9] L. Zhou and Z. Haas, "Securing ad-hoc networks," IEEE Netw., vol. 13, no. 6, pp. 24–30, Nov./Dec. 1999.

[10] M. Zapata and N. Asokan, "Securing ad hoc routing protocols," in Proc. ACM Workshop Wireless Secur., 2002, pp. 1–10.

[11] 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.

[12] R. Rivest, A. Shamir, and L. Adleman, ―A method for obtaining digital signatures and public-key cryptosystems, Commun. ACM, vol. 21, no. 2,Feb. 1983, pp. 120–126.

[13] Botan, A Friendly C ++ Crypto Library. [Online]. Available: http:// botan.randombit.net/

[14] 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.