Survey on IDS for Addressing Security Issues of MANETS

Agna Jose E.[1], Manu M.R.[2]
[1]Computer science and engineering, Royal college of engineering, India
[2]Computer science and engineering, Royal college of engineering, India

ABSTRACT **:** *Applications based on the mobility and scalability is one of the common phenomenon for current wireless network. Among all the up to date wireless networks, Mobile Ad hoc Network (MANET) is one of the most important and unique applications. MANET consists of mobile nodes which are free to move arbitrarily. MANETs are highly vulnerable for passive and active attacks because of their open medium, rapidly changing topology, lack of centralized monitoring. However, the open medium and wide distribution of nodes in MANET leave it vulnerable to various means of attacks. It is crucial to develop suitable intrusion detection scheme to protect MANET from malicious attackers. In this paper we describe different intrusion detection systems on manet.*

Keywords *- Enhanced Adaptive Acknowledgment Intrusion Detection System, Mobile AdHoc Network, Digital Signature.*

1. INTRODUCTION

Adhoc networks typically refer to any set of networks where all devices have equal status on a network and are free to associate with any other adhoc network devices in link range [5]. One of the classification of adhoc network is Mobile Adhoc Network(MANET). 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 [3].

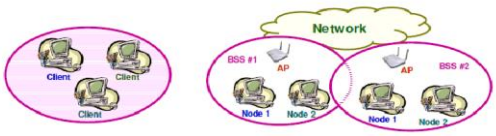

Figure 1.1 AdHoc network [3]

MANETS become more popular because of its attractive characteristics such as mobility and scalability [3]. Now a days all the people like mobile devices like cell phones, laptops etc. This is not only because of these 2 characteristics. Manets have some more advantages. Manets have much more improved technology and reduced cost. Manet is a self configuring network without the help of a fixed infrastructure or centralized management [3].

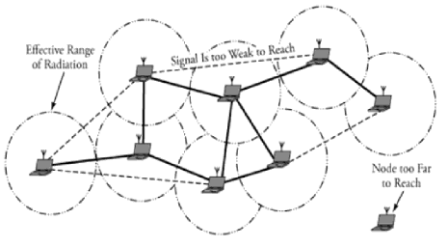

Figure 2.2 a typical MANET [3]

We have 2 types of networks, Single hop and Multihop. In single hop network, all nodes within the Same radio range communicate directly with each other. On the other hand in a multihop network, nodes rely on other intermediate nodes to transmit if the destination node is out of their radio range. Manet supports both types of networks [3].

There are mainly two types of network layer attacks in MANETs, namely active attack and passive attack. For passive attacks attackers attempt to seek some valuable in formations through traffic analysis. So this will not disturb the operation of the routing protocol. Eavesdropping, Traffic Analysis and Location Disclosure are some examples for passive attack. In manet we are using wireless links. So messages will sent by a node can be heard by every other devices with in the radio range and have transceiver with the device. This type of attack is called eavesdropping. By traffic analysis attacker can get the information about the transmitted data and characteristics of transmission. For active attacks, intruders had done activities like modifying, injecting, forging, fabricating or dropping data or routing packets etc. This will disturb the network operations. So it may become severe and degrade the network performance. Sleep Deviation, Black Hole, Gray Hole, Rushing, Sybil, Malicious Packet Dropping are different types of active attacks.

We can protect our mobile nodes from attackers by providing two wall of defense. First wall is Encryption and Authentication and Second wall of defense is Intrusion detection. Encryption and authentication were first brought in to consideration and many techniques have been proposed and implemented.

Cryptography technique has a long and fascinating history. From 4,000 years ago by the Egyptians, to the two world wars in the twentieth century, the cryptography technique has been widely served as a tool to protect secrets. With the development of Internet, the security of communication has become more important than ever. Many researchers and scientists have contributed their countless time and efforts in this area since then. Cryptographic techniques are typically divided into two generic types: symmetric-key and public-key.

For symmetric-key, the encryption key and decryption key are usually identical. The keys are used as a shared secret between two or more parties. The network can only choose a shared key to encrypt or decrypt message when the participants exchanged this key through a secure channel. Alice is the sender party while Bob is the receiver party. In order to communicate over unsecure channel, both parties have to exchange the shared secret key *k* through a secure channel first. In MANET, due to its open medium, attackers can easily capture one node and duplicate multiple malicious nodes. In the case of symmetric-key encryption, all nodes shared the same secret key. Compromised one node could well lead to a collapse of the entire network.

For public-key encryption, the encryption key (public key) and decryption key (private key) are different. Receiver holds both the public key and private key. The public key can be revealed to sender via an unsecured channel, as the secret cannot be known without the according private key. However these applications are not sufficient. If we have the ability to detect the attacks, we can stop it from doing any damage to the system or any data. Here is where the intrusion detection system comes in.

2. Literature Review

MANET IDSs without properly considering mobility cause different security issues. Most previous work on MANET IDSs adopts mobile speed and node pause time to capture the information on mobility on detection algorithms. We have observed that mobile speed alone is not an accurate measurement. The extraction of a common parameters in mobile devices are very important. Moving speed is not capable in measuring the performance of MANET. IDSs-hop change rate, which dynamically reflects different mobility factors. However, mobile speed alone cannot tell IDS how fast the hop changes are and the parameters setting based on mobile speed will not be correct [19].

DSR is an on-demand routing protocol and Every packet has a routing path. Which consist of the addresses of nodes that have agreed to participate in routing the packet. The word "on-demand" reffer route paths are discovered when a source need to sends a packet to a destination but which has no path. We divide DSR into two main functions: route discovery and route maintenance.

Node S (the source) wishes to communicate with node D (the destination) but does not know any paths to D. S initiates a route discovery by broadcasting a ROUTE REQUEST packet to its neighbor nodes that contains the destination address D. The neighbours append their own addresses to the ROUTE REQUEST and rebroadcast this request. This will continues until request packet reaches destination. After that Destination must send a route reply packet to Source. This will provide discovered route. Since there can be many routes from a source to the destination, a source may receive multiple route replies from a destination. DSR keeps these routes in a route cache for future use. The second function is route maintenance like. A link break occurs when two nodes on a path are not in transmission. If an intermediate node detects a link break when forwarding it sends back a message to the source notifying that link break. The source must try another path or do a route discovery if it another path.

Sergio Marti, T.J. Giuli, Kevin Lai, and Mary Baker describe two techniques [1] called watchdog and pathrater that improve throughput in an ad hoc network in the presence of nodes that agree to forward packets but fail to do so. To solve this problem, we propose categorizing nodes based upon their dynamically measured behaviour. We use a watchdog that identifies misbehaving nodes and a path-rater that helps routing protocols avoid these nodes. Watchdog maintaining a buffer of recently sent packets and comparing each overheard packet with the packet in the buffer to check if there is a match. If so, the packet in the buffer is removed. If a packet has remained in the buffer for longer than a certain timeout, the watchdog increments a failure count for the node responsible for forwarding on the packet. If the count exceeds a certain threshold , it determines that the node is misbehaving and sends a message to the source to inform it of the misbehaving node.

The watchdog technique has 6 weaknesses also. DSR with the watchdog has the advantage that it

can detect misbehavior at the forwarding level and not just the link level. Watchdog's weaknesses are that it might not detect a misbehaving node in the presence of ambiguous collisions, false misbehavior, collusion, receiver collisions, limited transmission power, and partial dropping.

The path-rater, check each node in the network and combines knowledge of misbehaving nodes with link reliability data to pick the route most likely to be reliable. Each node maintains a rating for every other node it knows about in the network. It calculates a path metric by averaging the node ratings in the path. We choose this metric because it gives a comparison of the overall reliability of different paths and allows path-rater to emulate the shortest length path algorithm when no reliability information has been collected, as explained below. If there are multiple paths to the same destination, we choose the path with the highest metric. Note that this differs from standard DSR, which chooses the shortest path in the route cache. Further note that since the Pathrater depends on knowing the exact path a packet has traversed, it must be implemented on top of a source routing protocol.

Many intrusion detection systems are tightly related to routing protocols, like Watchdog/Pathrater and Route guard. These solutions include intrusion detection (Watchdog) and response (Pathrater and Routeguard). Each node has individual watchdog .Which is based on overhearing. So each node can detect the malicious action of its neighbors and report other nodes. If the node that is overhearing and reporting itself is malicious, then it can cause serious impact on network performance. Sergio Marti, T.J. Giuli, Kevin Lai, and Mary Baker overcome the weakness of Watchdog and introduce an intrusion detection system [2] called ExWatchdog. The main feature of the proposed system is its ability to discover malicious nodes which can partition the network by falsely reporting other nodes as misbehaving and then proceeds to protect the network. The intrusion detection system ExWatchdog by extending Watchdog proposed in [1]. The solution is particularly aims at solving weaknesses presented by Watchdog: a malicious node falsely reports other nodes as misbehaving. Each node maintains a table that records the number of packets the node sends, forwards or receives respectively. When receives a report about misbehaving nodes, the source of a communication can send a message to the destination to check if the sums of packets the two parts stores are equal. If they are equal, then the real malicious node is the node that reports others nodes as misbehaving. Otherwise, nodes being reported malicious do misbehave.

Compared to Watchdog, solution has the same advantages. At the same time, it solves one big weakness: false misbehavior. It can detect if nodes falsely report other nodes as misbehaving. As stated earlier, false reporting may result in network partition and further decrease network performance. However, there is limitation in our solution. 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. For this case, we do not and cannot take any action because we do not know who lies and cannot either check. The Route guard decreases rating of neither the reporting node nor the reported node.

Kejun Liu, Jing Deng Pramod K. Varshney and Kashyap Balakrishnan propose [3] the 2ACK scheme to mitigate the adverse effects of misbehaving nodes. The basic idea of the 2ACK scheme is that, when a node forwards a data packet successfully over the next hop, the destination node of the next-hop link will send back a special two-hop acknowledgment called 2ACK to indicate that the data packet has been received successfully. Such a 2ACK transmission takes place for only a fraction of data packets, but not all. Such a "selective" acknowledgment1 is intended to reduce the additional routing overhead caused by the 2ACK scheme. Judgment on node behavior is made after observing its behavior for a certain period of time.

The 2ACK and the TWOACK schemes have the following major differences: The receiving node in the 2ACK scheme only sends 2ACK packets for a fraction of received data packets, while, in the TWOACK scheme, TWOACK packets are sent for every data packet received. Acknowledging a fraction of received data packets gives the 2ACK scheme better performance with respect to routing overhead. The 2ACK scheme has an authentication mechanism to make sure that the 2ACK packets are genuine. The Selective TWOACK (S-TWOACK) scheme proposed in is different from 2ACK as well. Mainly, each TWOACK packet in the S-TWOACK scheme acknowledges the receipt of a number of data packets, but a 2ACK packet in the 2ACK scheme only acknowledges one data packet. With such a subtle change, the 2ACK scheme has easier control over the trade-off between the performance of the network and the cost as compared to the S-TWOACK scheme.

The watchdog detection mechanism in has a very low overhead. Unfortunately, the watchdog technique suffers from several problems such as ambiguous collisions, receiver collisions, and limited transmission power. The main issue is that the event of successful packet reception can only be accurately determined at the receiver of the next-hop link, but the watchdog technique only monitors the transmission from the sender of the next-hop link. Noting that a misbehaving node can either be the sender or the receiver of the next-hop link, we focus on the problem of detecting misbehaving links instead of misbehaving nodes. In the next-hop link, a misbehaving sender or a misbehaving receiver has a similar adverse effect on the data packet: It will not be forwarded further. The result is that this link will be tagged. This approach discussed here significantly simplifies the detection mechanism. The 2ACK scheme is a network-layer technique to detect misbehaving links and to mitigate their effects. It can be implemented as an add-on to existing routing protocols for MANETs, such as DSR. The 2ACK scheme detects misbehaviour through the use of a new type of acknowledgment packet, termed 2ACK. A 2ACK packet is assigned a fixed route of two hops (three nodes) in the opposite direction of the data traffic route.

Elhadi M. Shakshuki, Nan Kang, and Tarek R. Sheltami proposed [4] EAACK is consisted of three major parts, namely, ACK, secure ACK (S-ACK), and misbehavior report authentication .

ACK(End to End acknowledgement scheme)

- Normal packet transmission done by this scheme
- If we send packet Pad1 from source S to destination D through A, B, C. Then...

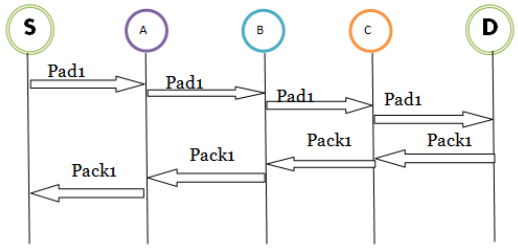

Figure 2.1 ack scheme

- If the acknowledgement packet received securely within a predefined time period send next packet.
- If the acknowledgement packet is not received securely within a predefined time period shifted the packet mode to S-ACK.

S-ACK (TWOACK acknowledgement scheme)

- Detect by acknowledging every data packet transmitted over every three consecutive nodes along the path from source to destination.
- Every node along the path need to send back a secure ack packet to the current node to the node which is 2hop away from it back.

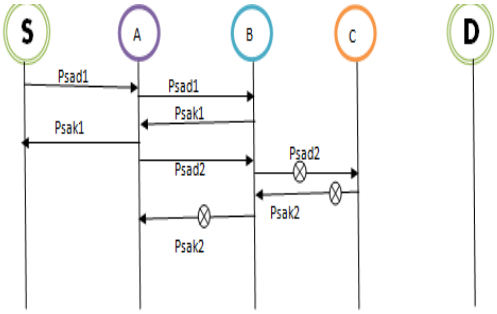

Figure 2.2 s-ack scheme

- If node A doesn't receive s-ack packet with in a predefined time period, both B and C are reported as malicious.
- Then misbehaviour report is generated by A is send to Source S.
- Then source switch to MRA scheme.

MRA(misbehaviour report authentication)

- Authenticate whether the destination node has received the reported missing packet through another route.
- For that, we first search for an alternative route to destination.
- Then sent a MRA packet from S to D through that alternative path.
- After receiving in the destination, it searches its local knowledgebase and compares if the reported packet was received.
- If it was already received, then it concludes that this report is false report and marks the node whoever generates this report as malicious.
- Then avoid the malicious node in future transmission.

In MANET we can find multiple paths between pair of nodes. By choosing an alternative route source can circumvent the misbehavior reporter node. When the node D receives an MRA packet, it look in to its local knowledge base and check if the reported packet was received. If it is received, then conclude that this report is a false misbehavior report and reporter, whoever generated this report

is marked as malicious node. Otherwise, report is trusted and accepted. By MRA scheme, EAACK can detect malicious nodes even in the presents of alse misbehavior report. Fig.2.1[4] shows the system flow EAACK scheme.

EAACK is an acknowledgment-based scheme. All parts of EAACK are acknowledgment-based detection schemes. So we must want to ensure that all acknowledgment packets are authentic and trusted. Otherwise all of the three schemes will be vulnerable. For ensure the integrity digital signature is included with EAACK.

Figure 2.3 system control flow [4]

Nan Kang, Elhadi M. Shakshuki and Tarek R. Sheltami describe Enhanced Adaptive ACKnowledgement version 2 [5] (EAACK2) scheme. This scheme is based on our previous research EAACK [4]. Compared to EAACK, EAACK2 advances in the following scenarios:

- Acknowledgement authentication: Prevents attackers from forging fake acknowledgement packet and thus conceive its malicious misbehavior.
- Packets integrity: Prevents attackers from contaminate packets in MANETs.

An improved IDS scheme for MANETs is proposed. Compared to the previous work, despite a slight increase in network overhead, EAACK2 not only achieves a better performance in the presence of forged acknowledgement packets, but also assures the packets integrity when potential attack occurs. Considering the consequences of smart attackers breaking down the entire network and the fact that military task are one of the most popular implementation of MANETs, we believe this trade-off between security and performance is worthwhile. So we are proposing a new technique called geographical routing. In this technique each node has some knowledge of its own position and of the position of the sink node, i.e., the node where the information needs to be delivered. Once a node has a packet to send, it sends it using some type of broadcast address while specifying its own location and the location of the intended destination. All active (listening) nodes in the coverage area will receive this packet and will assess their own priority in trying to act as a relay, based on how close they are to the destination.

3. Performance Evaluation

In order to measure and compare the performance of these schemes, we continue to adopt the following two performance metrics:

• Packet Delivery Ratio (PDR): PDR defines the ratio of the number of packets received by the destination node and the number of packets sent by the source node.

• Routing Overhead (RO): RO defines the ratio of the amount of routing-related transmissions (RREQ, RREP, RERR, ACK, S-ACK and MRA).

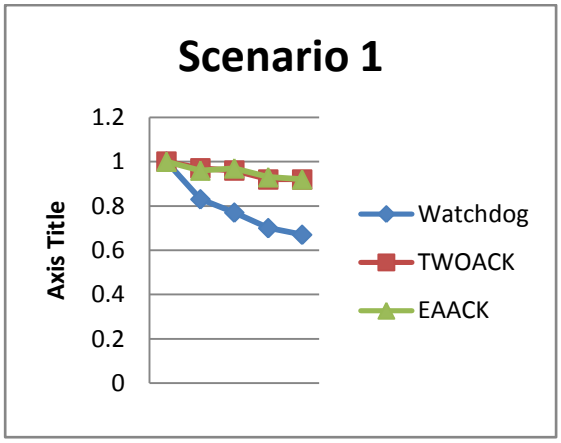

Figure 3.1 packet delivery ratios

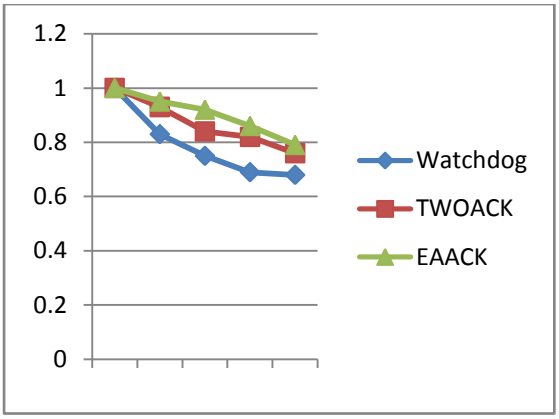

Figure 3.2 routing overhead

4. Conclusion

As MANETs become widely used, the security issue has become one of the primary concerns. For example, most of the routing protocols proposed for MANETs assume that every node in the network is cooperative and not malicious. Therefore, only one compromised node can cause the failure of the entire network. There are both passive and active attacks in MANETs. For passive attacks, packets containing secret information might be eavesdropped, which violates confidentiality. Active attacks, including injecting packets to invalid destinations into the network, deleting packets, modifying the contents of packets, and impersonating other nodes violate availability, integrity, authentication, and non-repudiation. Proactive approaches such as cryptography and authentication were first brought into consideration, and many techniques have been proposed and implemented. However, these applications are not sufficient. If we have the ability to detect the attack once it comes into the network, we can stop it from doing any damage to the system or any data. Here is where the intrusion detection system comes in. Although the watchdog is used in all of the above IDS, the authors in [1] have pointed out that there are several limitations. The watchdog cannot work properly in the presence of collisions, which could lead to false accusations. Moreover, when each node has different transmission ranges or implements directional antennas, the watchdog could not monitor the neighborhood accurately. All of the above IDS's presented are common in detecting selfish nodes. However, CORE doesn't detect malicious misbehaviors while the others detect some of them, i.e., unusually frequent route update, modifying header or payload of packets, no report of failed attempts, etc. As the use of mobile ad hoc networks (MANETs) has increased, the security in MANETs has also become more important accordingly. Historical events show that prevention alone, i.e., cryptography and authentication are not enough; therefore, the intrusion detection systems are brought into consideration. Since most of the current techniques were originally designed for wired networks, many researchers are engaged in improving old techniques or finding and developing new techniques that are suitable for MANETs.

With the nature of mobile ad hoc networks, almost all of the intrusion detection systems (IDSs) are structured to be distributed and have a cooperative architecture. The number of new attacks is likely to increase quickly and those attacks should be detected before they can do any harm to the systems or data. Hence, IDS's in MANETs prefer using anomaly detection to misuse detection [7]. Some techniques are proposed to implement on top of the existing protocols, others are proposed as independent modules to be added on mobile nodes. An intrusion detection system aims to detect attacks on mobile nodes or intrusions into the networks. However, attackers may try to attack the IDS system itself [5]. Accordingly, the study of the defense to such attacks should be explored as well. Many researchers are currently occupied in applying game theory for cooperation of nodes in MANETs as nodes in the network represent some characteristics similar to social behavior of human in a community. That is, a node tries to maximize its benefit by choosing whether to cooperate in the network.

References

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

[2] 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.

[3] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An acknowledgment-based approach for the detection of routing misbehavior in MANETs," IEEE Trans. Mobile Comput., vol. 6, no. 5, pp. 536–550, May 2007.

[4] EAACK – A Secure Intrusion Detection System for MANETs, Elhadi M. Shakshuki, Nan Kang, and Tarek R. Sheltami, 2012.

[5] 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.

[6] A.Menezes, P. van Oorschot, and S. Vanstone, Handbook of Applied Cryptography. Boca Raton, FL: CRC, 1996, T-37.

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

[8] A.Patwardhan, J. Parker, A. Joshi, M. Iorga, and T. Karygiannis, "Secure routing and intrusion detection in ad hoc networks," in Proc. 3rd Int. Conf.Pervasive Comput. Commun., 2005, pp. 191–199.

[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] 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.

[11] B. Sun, "Intrusion detection in mobile ad hoc networks," Ph.D. dissertation, Texas A&M Univ., College Station, TX, 2004.

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

[13] R. Rivest, A. Shamir and L. Adleman. A Method for Obtaining Digital Signatures and Public-key Cryptosystems. Communications of ACM 21 (2): 120-126, 1978.

[14] W. Diffie and M. E. Hellman. New Directions in Cryptography. In 1976 IEEE Transactions on Information Theory, IT-11: 644- 654, 1976.

[15] Nat. Inst. Std. Technol., Digital Signature Standard (DSS) Federal InformationProcessing Standards Publication, Gaithersburg, MD, 2009, Digital Signature Standard (DSS).

[16] A.Singh, M. Maheshwari, and N. Kumar, "Security and trust management in MANET," in Communications in Computer and Information Science, vol. 147. New York: Springer-Verlag, 2011, pt. 3, pp. 384–387.

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

[18] 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.

[19] Liu, Kejun."Detecting Routing Misbehavior In Mobile AdHoc Network."(2006).