Acknowledgment based Intrusion Detection System for MANET

Ms. Midhukrishna K.
M.Tech Student
Department of Computer Science & Engineering
Thejus Engineering College, Thrissur, India

Abstract— MANETs has become one of the major research topics nowadays due to the day by day increment of mobile users. The scalability that is provided by MANETs made it possible for many applications such as military, emergency operations, traffic analysis etc. But the flexibility in such environments has the risk of security. In such cases an efficient intrusion detection method is needed in order to transmit a data securely. This paper analyses intrusion detection systems based on DSR. The main task of this method is to identify the node which acts as an intruder. Compared to single path DSR, the proposed method improves network lifetime due to the use of multipath protocol.

Key words: Mobile Ad-hoc Network (MANET), TWOACK, DSR, Adaptive Acknowledgement, DSR, Digital Signature

I. INTRODUCTION

MANET is diverse from infrastructure network and centralized access point. Mobile Ad hoc Networks (MANETs) have been used in a varied range of applications such as disaster assistance, monitoring of environment and vehicular networks, traffic analysis, campus networks, Military applications etc. It also includes the wide space of vulnerabilities due to their challenges and issue, which makes the degradation of the network. Absence of reliability of nodes due to its mobility and changing topology, hence it is more prone to malicious attacks. Lack of security in network leads the intruder to interrupt the transmission of data. Energy Consumption affects the transmission of data in between every mobile node. The major challenge includes the routing in mobile ad hoc networks since the frequent change of topology which makes the difficult task to route the packets towards the adjacent nodes in the network Authentication. Encryption can be used as the primary defense. But those techniques lack the well-organized defense to the attack, hence to overwhelm the attacks and challenges in MANET intrusion detection systems. An ID is a software or system that analyses a network and check whether any intrusion happened. IDS facilitates the intrusion detection process, initial responsibility of IDS is to detect undesirable and intruder activities. It is the defensive mechanism in the mobile ad-hoc network which provides the secured communication in between the mobile nodes. In fixed networks, intrusion detection and system (IDS) acts as a second layer of defense beyond a firewall.

The recent methods to detect malicious nodes can be classified into three categories: Credit-based, reputation-based and acknowledgement-based. Reputation based uses a Watchdog for monitoring the system. Watchdog overhears the transmission of packets to next nodes. In credit based technique incentives are provided for each node for providing services to other nodes. Virtual (electronic) currency is used to achieve this specific goal. Packet trade model and packet purse models are some among those. Acknowledgement based scheme rely on the concept that ensures the delivery of packets. But the problem with ACK based method is the overhead due to continuous reception of acknowledgement packets.

A. Security Issues in MANET

Security dependably assumes a fundamental part to distinguish different sorts of assaults, security dangers and distinctive vulnerabilities exhibit in a framework. Helplessness could be a shortcoming in security arrangement of any system. A specific framework might be inclined to unapproved access to control information on the grounds that the framework does not confirms a client's realness before allowing it to access into the system. Remote specially appointed system like MANET is more powerless than wired system. A portion of the significant issues in regards to vulnerabilities in versatile specially appointed system are as per the following:

B. Lack of Centralized Management

There isn't any idea of concentrated planning framework in the versatile impromptu system. As a result of the nonappearance of focal administration framework it is extremely intense undertaking to identify assaults exhibit in the system, since it is difficult to watch the activity in a versatile and huge specially appointed system. Absence of brought together planning framework may soften trust among hubs up the system.

C. Resource Availability

Accessibility of assets is a major issue in MANET. Setting up secure correspondence way in such unique system and shield the system from different assaults, winds up to the improvement of various security methodologies and frameworks. Helpful specially appointed system dependably allows advancement of self-composed security frameworks.

D. Scalability

As a result of the moving idea of hubs, period of specially appointed system changes constantly. Accordingly adaptability is an essential issue with respect to security of impromptu system. Consequently security framework ought to have the capacity to deal with an extensive scale organize and in addition little ones.

E. Cooperativeness

Some steering calculation for MANET like AODV typically expect that hubs are agreeable in nature and non-assailant. Therefore an assailant hub may wind up noticeably principle steering operator effectively and control arrange works as not following the convention rules.

F. Dynamic Topology

Dynamic nature and mobile hubs relationship can break the trust between hubs. The trust of a hub can likewise be aggravated if couple of hubs are distinguished as concurred.

This dynamic or alterable nature can be better ensured with disseminated and helpful security frameworks.

G. Limited Power Supply

The power supply for any node in mobile ad- hoc network could behave in a selfish manner once it's realized that there is limited power supply.

In this paper, a new scheme is proposed against packet drop attack and finds out the misbehaving node and removes all paths including the malicious one. DSR is the protocol behind the method. Moreover, MAC is used in order to identify the sender of packet.

The rest of this paper is organized as follows. In the coming section literature survey is summarized. In section 3, we propose our scheme in detail. Later, section 4 describes performance analysis of some existing methods on intrusion detection. Conclusion and future work are written in last 2 sections.

II. RELATED WORK

Due to the limitations of MANET routing protocols all nodes in MANET assumes that other nodes cooperate in order to transmit data. To solve this problem, efficient IDS should enhance security of MANETs. This section describes some closely related topics on IDS.

Ramasamy murugan and Arumugam shanmugam proposed a method [4] which detects and isolates the misbehaving nodes and find the number of misbehaving nodes in the route that is greater than the minimum count. This scheme maintains a good packet delivery ratio with reduced packet drop and overhead. In this method group of nodes are divided into sets. Suppose there are 2 sets and source node of the 1st set gets an acknowledgement from destination node after reception of data packet. The destination node of 2nd set must send the acknowledgment to the source node of 1st one. For avoiding delay and overhead, this scheme proposes a detection timer. Timer has specific time interval assigned to it. Source starts its timer when it forward packet. The destination node is checked when detection timer over. Then a negative acknowledgement will be sent to source node If the forward count is below threshold. Else the positive acknowledgement (PACK) is sent. This process is repeated.

"Watchdog" [5] technique proposed by Marti et al. It consisted of two parts, Watchdog and Pathrater. Watchdog serves as IDS for MANETs. Watchdog detects misbehaving nodes in network. Pathrater technique responds to these nodes by helping the routing protocol to avoid these nodes. Watchdog is the basic one among intrusion detection systems in MANETs. But it does not work efficiently in the presence of ambiguous collisions.

Lightweight sybil attack detection in MANETs [6], a Sybil attacker can disrupt location-based or multipath routing by participating in the routing, giving the false impression of being distinct nodes on different locations or node-disjoint paths. In reputation and trust-based misbehavior detection schemes, a Sybil node can disrupt the accuracy by increasing its reputation or trust and decreasing others' reputation or trust by exploiting its virtual identities. In wireless sensor networks, a Sybil attacker can change the whole aggregated reading outcome by contributing many times as a different node. In voting-based schemes, a Sybil attacker can control the result by rigging the polling process using multiple virtual identities. In vehicular ad hoc networks, Sybil attackers can create an arbitrary number of virtual nonexistent vehicles and transmit false information in the network to give a fake impression of traffic congestion in order to divert traffic. Therefore, Sybil attacks will have a serious impact on the normal operation of wireless ad hoc networks. It is strongly desirable to detect Sybil attacks and eliminate them from the network. The traditional approach to prevent Sybil attacks is to use cryptographic-based authentication or trusted certification. However, the approach is not suitable for mobile ad hoc networks because it usually requires costly initial setup and incurs overhead related to maintaining and distributing cryptographic keys. On the other hand, received signal strength (RSS) based localization is considered one of the most promising solutions for wireless ad hoc networks. However, the approach requires extra hardware, such as directional antennae or a geographical positioning system (GPS).

Michiardi and Molva [7] proposed CORE (Collaborative Reputation Mechanism) to detect and isolate selfish nodes. CORE stimulates node cooperation by a collaborative monitoring technique and a reputation mechanism. Each node computes a reputation value for every neighbour that differentiates between subjective reputation (observation), indirect reputation (positive reports by others) and functional reputation (take-specific behaviour). Two basic components for the CORE mechanism are reputation table and watchdog mechanism [5]. The watchdog mechanism is used to detect misbehaviour nodes. The reputation table is a data structure stored in each node. Each row of the table consists of four entries: the unique identifier of the entity, a collection of recent subjective observations made on that entity's behaviour, a list of the recent indirect reputation values provided by other entities and the value of the reputation evaluated for a predefined function. The CORE scheme involves two types of protocol entities, a requestor and one or more providers that are within the wireless transmission range of the requestor. If a provider refuses to cooperate (the request is not satisfied), then the CORE scheme will react by decreasing the reputation of the provider. Route tables are updated in two different situations: During the request phase of the protocol and during the reply phase corresponding to the result of the execution. In the first case only the subjective reputation value is updated while in the second case, only the indirect reputation value is updated. The advantages of CORE mechanism are to prevent the DOS attacks and it is impossible for a node to maliciously decrease another node's reputation because there is no negative rating spread between nodes. The limitations of CORE suffers from spoofing attack and it cannot prevent colluding nodes from distribute negative reputation.

"TwoAck [8]" method uses new acknowledgement packet termed as TWOACK to detect misbehaviors. Figure 1 illustrates the TWOACK scheme. Suppose A, B and C are three nodes along a route from source to destination. Node A node sends a packet to node B and then B forwards it to node C but A doesn't know whether node B forwarded packet or not. Then node C generates a TWOACK packet and sends it

to B then to A. Now node A confirm that node C successfully received the packet. Drawback of TWOACK scheme is the continuous acknowledgement messages. Because it creates high network overload.

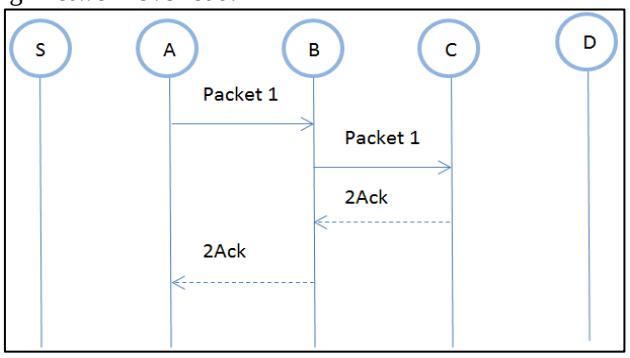

Fig. 1.2: Ack Scheme

III. METHODOLOGY

The proposed system consists of 3 schemes. Aack, ThAck, E2EAck.

A. Aack

Aack is an adaptive acknowledgement scheme. It is basically an end to end ack based method. The method mainly aims to reduce network overload. Fig 2 shows the general working of Aack mode.

In Aack mode node S initiates data transmission. S sent data packet onto A, Then a transfer it to B later to C, X and D. While the message reaches at destination D successfully, D sent Aack packet back to source. But this method explains the case only if all nodes are normal. If the source node doesn't get the Aack in a predefined time, it will sitch on to next mode called Thack.

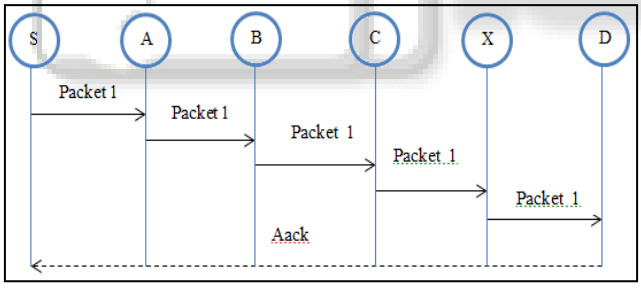

Fig. 2: Aack Mode

B. Thack

Thack is almost similar to TwoAck. The only difference is that instead of taking 2 hop neighbor Thack considers three hop neighbours. Fig 3 gives a complete structure of Thack. In the figure, S sents a data packet to A, Later A forward the packet to B, then to C. C is the 3 hop neighbor of S. So when data receive at C, it will sent a Thack message back to node which initiated transfer. If Thack doesn't received it will move onto next state called E2EAck.

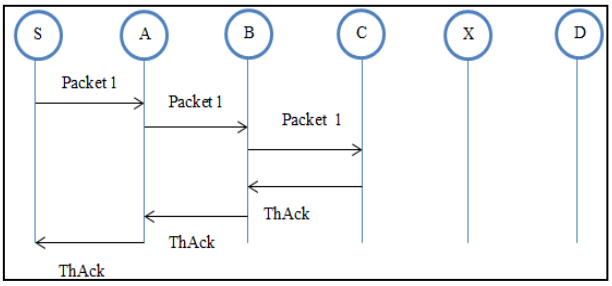

Fig. 3: Thack Mode

C. E2EAck

E2EAck is an end to end acknowledgement based scheme. The main concept of the method is proving honesty of each node. E2EAck detects packet dropping. Before moving onto the concept, some assumptions are taken. Each node has a unique id that can't be spoofed. There will be malicious node and suspicious node. Suspicious is the one that is marked as malicious by other one.

Each node maintains two tables. First table contains the fields such as id, public key, malicious flag. Malicious flag will be initially zero, it will be updated to one if it is shown that the node is malicious. The second table contains five fields named packet, id, Tdelay, suspicious node, Tdelay is the time between sending a packet and receiving its Ack. Ack packet contain 4 fields. ID (received packet id), Digital sign, ErrorReportFlag (0 if it is Ack and 1 if it is an error report) When a node the path receives a packet while transmitting data, the node which get the message will set a timer. Before the timer reaches 0, it's its Ack should get. Else each node prove its honesty. Honesty of a node can be proved in 2 ways.

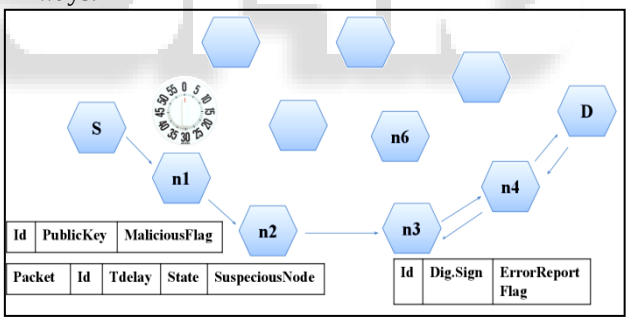

Fig. 4: Basic E2EAck

First method is forwarding data packet correctly and the next one is broadcasting of data packet to its own neighbours. If a node doesn't prove its honesty it will be considered as malicious. If a packet with error report flag=1 reaches source node, it will extract sender index and calculate new time delay. If Ack get successfully, the entry for that node will be deleted. There are 2 chances for proving a node's honesty. At the first chance if acknowledgement is not received in particular time, the source node sets the node next to it as suspicious and broadcast it to neighbours. The suspected node also gets the message and it understands that it is marked as malicious. So it will prove its honesty via second chance.

Second chance means, the suspected node prove the evidence that it has transferred data packet correctly. For this it will find another route to source and sent the time and other related information to source. Hence source understands that suspected node is actually normal. So source remove the

suspected normal. The node which doesn't sent the evidence, it is clear that, that particular node is malicious.

1) Suspicious Node & Malicious Node

When a packet with ErrorReportFlag equal to one reaches the source node, this node finds the table entry of the packet (using the PacketID) and sets State (going to the second waiting) and extracts the sender index on the path of the original packet header to find the suspicious node(the node after the sender) and puts the suspicious node in''quarantine'' fact, when a node receives a broadcast data packet and detects its ID as the next node on the path, the node understands that the neighbors and the source node add its name as a suspicious node. Therefore, if it receives an evidence (the ACK packet from the destination node or a route error packet), it must broadcast the evidence to the neighbors (with TTL = 2 to cover all neighbors that are in the second waiting time) and sends it to the source node in a new route that does not contain the reporter node (to prevent slander attacks).However, if the second waiting time is finished and the source node, the reporter node, and the reporter node's neighbors do not receive the ACK packet (or a route error packet), they consider the quarantined/suspicious node as a malicious node by setting the MaliciousFlag of this node on the table and remove all paths in their caches that contain the malicious node. Therefore, when a new packet is needed to transmit to the same destination, a new route request should be sent by the source node if the cache does not have any route to this destination. Note that if the source node had a packet to send to the destination node during the second waiting time, it would not use a route that contains a suspicious node. By this way we can decrease the number of dropped packets. However, we cannot remove a path that contains a suspicious node after the first waiting because this node may be detected as a safe node before the end of second waiting time. Because the reporter node's neighbors are the one-side neighbors of the malicious node, the advantages of knowing a malicious node by the reporter node's neighbors are:

1) If they receive a data packet and detect a malicious node as the next node on the path, they create a route error packet and send it back to the source node.
2) If they receive a route request packet with a malicious node on the path, they will drop this route request packet to prevent establishing a new route containing the malicious node.

To decrease the routing overhead, two updates can be done when the first deadline is reached and when the broadcast packet must be sent.

1) Node n2 must send an empty packet to node n3 before the deadline is reached. In this way if the link n2–n3was broken, n2 would receive a route error report from its MAC layer. Therefore, n2 can send back a route error packet and will not broadcast to get signatures.
2) When the deadline is reached, node n2 sends the data packet as a broadcast packet (with TTL = 1).

The neighbors must send back a packet that contains their digital signatures. It is better to send back this packet to n2 as a broadcast packet (destination IP address = n2, destination MAC address = BROADCAST).The neighbors should wait for a constant time (except n3) and then wait for a random time, to send their packets. If they see the signed packet of n3 (in the constant waiting time), they will not need to send their signatures because n3 confessed by sending this signed packet so they do not need any witnesses. If they do not see the packet of n3, after a random waiting time (random waiting time decreases the probability of packet collisions) they send signed packets provided they do not see more than a pre-defined number of signed packets of the neighbors. In fact, the pre-defined number depends on the required security level. To have a high-level of security, affidavits (signed packets)of all neighbors can be used.

D. Timeout Threshold

Timeout threshold is very significant element and it affects the accuracy of our system. If threshold is a large value, it will be a chance to nodes to make issues in a network. If it is too small, it will reduce performance of network. The time out for TWOACK has been experimentally calculated and its value is

$$TAckTout = 0.2s \quad (1)$$

Based on threshold of TACK, timeout threshold for Aack is

$$AackTout=(TAckTout/2)*number\ of\ hops \quad (2)$$

The threshold for ThAck is calculated according to (3)

$$ThAckTout=(TAckTout/2)*3 \quad (3)$$

IV. ANALYSIS OF METHODS

	A3Ack	E2EAck	EAAck
Packet delivery ratio	Better than EAAck	High	High
Routing overhead	High	Less than other methods	High
Delay	High	Less than other	High
Throughput	High	High	Low
Malicious node detection ratio	Low	High	Higher than A3Ack
Number of false alarm	High	Low	Low

Table 1: Comparative Study of Similar Methods

Table gives comparative study of different acknowledgement based methods. Packet delivery ratio of A3Ack [1] is better than EAAck [2] scheme due to frequent acknowledgement sending mechanism but the overhead is high in A3Ack and EAAck.E2EAck has less delay when compared to other two methods. Malicious nodes can be detected efficiently in E2EAck which increases the throughput.

REFERENCES

[1] Sheltami, Tarek, basabaa, Abdulsalam & Shakshuki, Elhadi, 2014. A3ACKs: adaptive three acknowledgments intrusion detection system for MANETs, Journal of Ambient Intelligence and Humanized Computing, pp. 611-620.
[2] Shakshuki, M. Elhadi, Kang, Nan & Sheltami, R. Tarek, 2013. EAACK—A Secure intrusion-detection system for MANETs, IEEE Transactions on industrial electronics, pp. 1089 - 1098.

[3] Heydari, Vahid, 2016. E2EACK: an end-to-end acknowledgment-based scheme against collusion black hole and slander attacks in MANETs, Journal of wireless networks, vol. 22, and pp. 2259–2273.
[4] Murugan, Ramasamy & Shanmugam, 2013. A timer based acknowledgement scheme for node misbehavior detection and isolation in MANET, International journal of network security, vol. 15, and pp. 241-247.
[5] Giuli, S.Marti & M. Baker, P. 2000. Mitigating routing misbehavior in mobile adhoc network, In: Proceedings of the 6th annual international conference on Mobile computing and networking, pp. 255-2653.
[6] Schweitzer, N. Stulman, A. Shabtai, A. & Margalit, R.D. 2017. Contradiction Based Gray-Hole Attack Minimization for Ad-Hoc Networks, IEEE Transactions on Mobile Computing, vol. 15, no. 1, and pp. 101 115.
[7] Buchegger, S. 2005. Self-policing mobile ad hoc networksby reputation systems, IEEE Communications Magazine, pp.56-63.
[8] Kejun, Liu, Deng, Jing, Varshney, K. Pramod & Balakrishnan, Kashyap basabaa, 2007. An acknowledgment-based approach for the detection of routing misbehavior in MANETs, Mobile computing, IEEE Transactions, pp. 536-550.
[9] Sun, B. 2004. Intrusion detection in mobile ad hoc networks, Ph.D. dissertation, pp. 404-410.
[10] Farokhtala, Ali & alizadeh, Mojtaba Vahid, 2015. DNACK: False Data Detection Based on Negative Acknowledgment and Digital Signature on Mobile Ad-hoc Network, Journal of Wireless Personal Communications, Volume. 83. pp. 1-15.
[11] Balakrishnan K. 2005, TWOACK: Preventing selfishness in mobile ad hoc networks, in proceedings of IEEE WCNC, vol. 15, pp. 2137–2142.
[12] Zhang, Y. Lazos, L. 2012, AMD: Audit-based misbehaviour detection in wireless ad hoc networks, IEEE Transactions on Mobile Computing, pp. 1-14.

