International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 11 Issue 6 –NOVEMBER 2014.

Collaborative Node Multi Level Hybrid Security Scheme for Intrusion Detection in MANETS

Katnekaluva Rajendra Babu*[1] and P. Namratha#[2]

* *M.Tech (CSE), Intell Engineering College, Affiliated to JNTUA, Andhra Pradesh, India*

#*Asst Professor, Dept of CSE, Intell Engineering College, Affiliated to JNTUA, Andhra Pradesh, India*

[1]rajendrababu556@gmail.com

[2]namratha.reddy535@gmail.com

Abstract— MANETS, a collection of wireless mobile nodes are capable of communicating with each other without any use of centralized administration. Although MANETS offer unrestricted mobility and connectivity to the users, they also act as routers for forwarding packets due to their limited transmission ranges. MANETS are also termed as Infrastructureless networking as the mobile nodes in the network dynamically establish routing among themselves in their own network on the fly. As all the signals go through a bandwidth constrained wireless links, it is more prone to physical security threats. These mobile nodes can roam independently and can move in any direction. Hence, any security solution with a static configuration would not be adequate for a dynamically changing topology. Due to the limitations of the most of the routing protocols devised for MANETS, leaves the attackers to have a significant impact on the network with just one or two compromising nodes. Hence, the IDS that are developed should provide enhanced security level for the network. If MANETS can detect the intruders as soon as they can enter the network we can eliminate the potential damages that can be caused by the compromised nodes at the initial levels itself.

Keywords: MANETS, receiver collisions, False misbehavior report, Hybrid IDS.

I. INTRODUCTION

MANETS is emerging research areas with practical applications. MANETS are vulnerable to attacks because of their dynamic topology, open medium, constrained capability. Also routing plays an important role in the security for the entire network. In MANETs, each node plays an important role not only as a host but also as a router. Each node participates in an adhoc routing protocol which allows discovering multi-hop paths within the network. Even though, this model provides flexible methods for communication, security is a critical issue. The possible attacks can range from passive eavesdropping to active interference. Any attacker can listen to or modify the traffic and might attempt to masquerade as one of the participants. Cryptography and certificate based authentication might be difficult in MANETS because of the absence of central support infrastructure.

The routing protocols designed for MANETS can exchange information between the source and the destination through the established routes. As all the messages are transmitted over the air any malicious intruder can give incorrect information by pretending as a legitimate change.

The transmission of the message completely relies upon the cooperative participation of all nodes. During this kind of transmission, a malicious node can block or modify the traffic by refusing the cooperation with other nodes which leads to the failure of the centralized intrusion detection algorithms.

As MANETS rely on their batteries for energy, an intruder can create a new type of DoS attack by forcing a packet to replay its packets to exhaust the energy levels. This can lead to the limited battery power and can lead to frequent disconnections from the network which makes hard to detect the anamolies.

To address all the above said problems [6], the intrusion detection schemes (IDS) should be enhanced. The proposed work implements a new intrusion detection system named Enhanced Adaptive ACKnowledgement (EAACK), which demonstrates higher malicious behavior detection rates without affecting the network performances.

II. EXISTING SYSTEM

The Intrusion detection schemes (IDS) act as a second layer in MANETS. The three main existing approaches are Watchdog, TWOACK and Adaptive ACKnowledgement (AACK) .

1. Watch dog scheme: This scheme proposed by Marti et al. aims to improve the throughput of the network with the

presence of malicious nodes. This scheme consists of two parts namely, Watchdog and Pathrater. The first part is responsible for detecting malicious misbehaviours by listening promiscuously to its next hop's transmission. If it overhears its next node fails to forward the packets further, the watchdog node increases its failure counter. If the failure counter exceeds a predefined threshold value the failed node is reported as misbehaving node. The second part of this scheme, Pathrater cooperates with the routing protocols to avoid the reported failed nodes in future transmission.

Eventhough Watchdog scheme is proved to be efficient in detecting malicious nodes rather than links; it fails to detect the misbehaving nodes in 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.

2) TWOACK: In order to overcome the limitations of the Watchdog scheme, many researchers proposed new approaches to solve these issues. TWOACK proposed by Liu et al. aims to resolve receiver collision and limited transmission power problems. TWOACK scheme aims at detecting misbehaving links by acknowledging every data packet transmitted 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 collaboratively work on routing protocols such as Dynamic Source Routing (DSR). Eventhough the TWOACK scheme successfully solves the receiver collision and limited transmission power problems posed by Watchdog. the acknowledgment process that is required in every packet transmission process adds a significant amount of an unwanted network overhead. Also due to the limited battery power of MANETs, the redundant transmission process can easily degrade the life span of the entire network.

3) AACK: This scheme proposed by Sheltami et al. is based on the previously discussed TWOACK scheme [4]. AACK is an acknowledgment-based network layer scheme, considered as a combination of TACK (identical to TWOACK) and an end-to-end acknowledgment scheme called ACKnowledge (ACK). 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.

At the same time, the functions of such detection schemes are largely dependent on the acknowledgment packets. Hence, it is crucial to ensure that the acknowledgment packets are valid and are also authentic. To address this concern, we adopt a digital signature scheme.

4. Digital Signature: A digital signature can be generalized as a data string, which associates a message (in digital form) with some originating entity, or an electronic analog of a written signature. Digital signature is a widely adopted approach to ensure the authentication, integrity, and nonrepudiation of MANETs.

These Digital signature schemes can be mainly divided into the following two categories.

1) Digital signature with appendix: Original message is required in the signature verification algorithm. Ex: Digital Signature Algorithm (DSA).

2) Digital signature with message recovery: This scheme does not require any other information besides the signature itself in the verification process. Ex: RSA.

Drawbacks of Existing System

- ❖ All the existing IDS schemes are vulnerable to
- ❖ Receiver collision.
- ❖ False Misbehavior Report attack.
- ❖ Limited Battery power
- ❖ Increased network overhead because of acknowledged packets.
- ❖ Excessive flooding of authentication control messages.

III. Proposed System

Of the many existing IDS in MANETS all are acknowledgement based. Hence, it is essential to check these acknowledgements are authentic.

The proposed implementation of EAACK is extended with the introduction of Digital Signature to prevent the network from forged acknowledgement packets. This work implements both DSA and RSA for digital signatures.

EAACK Approach is designed to tackle three of the six weaknesses of Watchdog scheme, false misbehavior, limited transmission power, and receiver collision.

EAACK scheme consists of three major parts, namely, ACK (Acknowledge), Secure ACK (S-ACK), and Misbehavior Report Authentication (MRA).To distinguish different packet types in different parts, a 2-bit packet header is introduced EAACK. In EAACK, 2 bit of the 6 bits packet type is used to flag different types of packets.

In this scheme, the link between each node in the network is assumed to be bidirectional. And for each communication process, both the source node and the destination node are not malicious. Unless specified explicitly, all acknowledgment packets are required to be digitally signed by its sender and verified by its receiver.

A. ACK

ACK is an end-to-end acknowledgment scheme acts as a part of the hybrid scheme in the proposed work aiming to reduce the network overhead when no network misbehavior is detected.

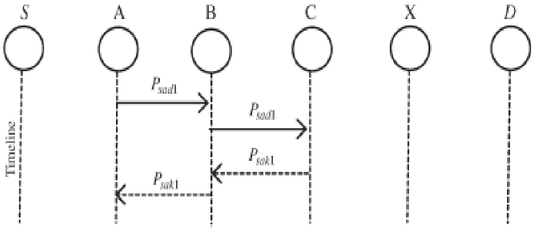

Fig1. Communication between nodes in ACK hybrid scheme

The working of ACK hybrid scheme can be best illustrated from the above figure explained as below:

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 the nodes S and D are successfully cooperative and if node D successfully receives Pad1, node D then sends back an ACK acknowledgment packet Pak1 along the same route but in a reverse order.

If within a predefined time span, if node S receives Pak1, then the packet transmission from node S to node D is successful. Else, node S will switch to S-ACK mode by sending out an S-ACK data packet to detect the misbehaving nodes in the transmitted route.

B. S-ACK

The S-ACK scheme proposed by Liu *et al.* is an improved version of the TWOACK scheme to let every three consecutive nodes work in a group to detect misbehaving nodes. The S-ACK mode is intended to detect misbehaving nodes in the presence of collision or limited transmission power. For every three consecutive nodes in the route, the third node is required to send an S-ACK acknowledgment packet to the first node.

In S-ACK mode, assuming the three consecutive nodes as F1, F2, and F3 works in a group to detect misbehaving nodes in the network

At the sender part node F1 first sends out S-ACK data packet Psad1 to node F2. Further, node F2 forwards this packet to node F3.

At the receiver side when node F3 receives Psad1, the third node in this three-node group, node F3 is required to send back an S-ACK acknowledgment packet Psak1 to node F2. Node F2 further forwards Psak1 back to node F1.

If node F1 does not receive this acknowledgment packet within a predefined time period, both nodes F2 and F3 are reported as malicious and a misbehavior report will be generated by node F1 and sent to the source node S.

Once EAACK receives the misbehavior report, it requires the source node to switch to MRA mode and confirm this report instead of immediately trusting as done in TWOACK scheme.

C. MRA

The MRA scheme is intended to resolve the weakness of Watchdog when it fails to detect misbehaving nodes with the presence of false misbehavior report. This false misbehavior report can be generated by malicious attackers to falsely report innocent nodes as malicious. With this attack the attackers can break down sufficient nodes and thus cause a network division. The crucial part of MRA scheme is to authenticate whether the destination node has received the reported missing packet through a different route.

The functionality of the MRA mode can be better explained as below:

As the initial step, the source node first searches its local knowledge base and seeks for an alternative route to the destination node.

If no route exists, the source node starts a DSR routing request to find another alternative route. By searching for an alternative route to the destination node, when the destination node receives an MRA packet, the source node searches its local knowledge base and compares if the reported packet has been received.

If it has already received the packet, then it is safe to conclude that the generated misbehavior report in S-ACK is a false misbehavior report and the node whoever has generated this report is marked as malicious node. Else, the misbehavior report is trusted and accepted.

D. Digital Signature

All three parts of EAACK IDS, ACK, S-ACK, and MRA, are acknowledgment-based detection schemes. All of these schemes rely on acknowledgment packets to detect misbehaviors in the network. Hence, it is extremely important to ensure that all acknowledgment packets in EAACK are authentic and untainted. If the intruders are smart enough to forge the acknowledgment packets, then all of the above said three schemes are made vulnerable.

To ensure the integrity of the EAACK IDS, it is required that requires all acknowledgment packets to be digitally signed before they are sent out at the source node and verified until they are accepted at the destination.

Using a preagreed hash function H for every message m a fixed-length message digest d can be computed as H(m) = d.

At the second level, the sender Alice tries to apply his own private key Pr−Alice on the computed message digest d. The result is a signature SigAlice, attached to message m and Alice’s secret private key given by

$$SPr-Alice\ (d) = SigAlice.$$

The sender Alice to always keeps her private key $P_{r-Alice}$ as a secret without revealing to ensure the validity of digital signature. If the attacker Eve gets this secret private key, then she can intercept the message and can easily forge malicious messages with Alice’s signature and send them to Bob. As these forged malicious messages are digitally signed by Alice, Bob views them as legitimate and authentic messages from Alice. Thereby, Eve can readily achieve malicious attacks to Bob or even to the entire network.

Once Alice sends a message m along with the signature SigAlice to Bob via an unsecured channel he then computes the received message m’ against the preagreed hash function H’ to get the message digest d’. This process can be generalized as

$$H(m') = d'.$$

(3) Bob can verify the signature by applying Alice’s public key Pk−Alice on SigAlice, by using

$$SPk-Alice\ (SigAlice) = d.$$

(4) If d == d’, then it is safe to claim that the message m’ transmitted through an unsecured channel is indeed sent from Alice and the message itself is not tampered or malicious.

ADVANTAGES OF PROPOSED SYSTEM

The proposed EAACK IDS scheme can detect higher-malicious behavior detection even in the presence of

1. Receiver collisions.
2. False Misbehavior reports.
3. Effective utilization of the network even in the presence of acknowledged packets.
4. Authenticity of data based on digital signatures.
5. Considerable amount of redundancy for ACK packets thereby reducing the network overhead.

IV. CONCLUSION AND FUTURE WORK

The simulated results for EAACK protocol demonstrates the positive performance against the Watchdog , TWOACK, AACK schemes for scenarios such as receiver collisions, limited transmission power report, false misbehavior report. In order to prevent the intruders from initiating the forged acknowledgement attacks, digital signatures are been incorporated which increases the network's PDR ration when there is a transmission of forged acknowledged packets.

The future research of this work can be carried out to solve the issues of reducing the network overhead that is caused by digital signatures, adopting a key exchange mechanism to eliminate the requirement of pre distributed keys.

REFERENCES

[1] EAACK—A Secure Intrusion-Detection System for MANETs Elhadi M. Shakshuki, Senior Member, IEEE, Nan Kang, and Tarek R. Sheltami, Member, IEEE Transactions on Industrial Electronics, March 2013.

[2] 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.

[3] 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.

[4] 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.

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

[6] Routing Security in Wireless Ad Hoc Networks, Hongmei Deng, Wei Li, and Dharma P. Agrawal, University of Cincinnati