Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 12, December 2013, pg.389 – 393

SURVEY ARTICLE

A Survey on Intrusion Detection System in Mobile Adhoc Networks

Arockia Rubi.S[1], Vairachilai.S[2]

PG Student[1], Assistant Professor[2]

Department of Computer Science and Engineering,
NPR College of Engineering and Technology,
TamilNadu, India.
E-Mail: arockiaruby.s@gmail.com

Abstract- The migration to wireless network from wired network has been a global trend in the past few decades. The mobility and scalability brought by wireless network made it possible in many applications. Among all the contemporary wireless networks, Mobile Ad hoc NETwork is one of the most important and unique applications. On the contrary to traditional network architecture, it does not require a fixed network infrastructure; In general, routing protocols for MANETs are designed based on the assumption that all participating nodes are fully cooperative. However, due to the open structure and scarcely available battery-based energy, node misbehaviours may exist. However, the open medium and wide distribution of nodes make MANET vulnerable to malicious attackers. In this case, it is crucial to develop efficient intrusion detection mechanisms to protect MANET from attacks.

Keywords- MANET; Intrusion Detection System; Digital Signature; Malicious nodes; Misbehaviour report; Acknowledgement

I. INTRODUCTION

Mobile Ad hoc NETwork (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 either directly or indirectly. MANET structure may vary depending on its application from a small, static network that is highly power constrained to a large-scale, mobile, highly dynamic network.

Every node works both a transmitter and a receiver. Nodes communicate directly with each other when they are both within the same communication range. Otherwise, they rely on their neighbors to relay messages. Industrial remote access and control via wireless networks are becoming more and more popular these days. One of the major advantages of wireless networks is its ability to allow data communication between different parties and still maintain their mobility.

This 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 nodes to rely data transmission. There are two types of MANETs: closed and open.

In a closed MANET, all mobile nodes cooperate with each other toward a common goal, such as emergency search/rescue or military and law enforcement operations. In an open MANET, different mobile nodes with different goals share their resources in order to ensure global connectivity. Some resources are consumed quickly as the nodes participate in the functions.

Battery power is considered to be more importance in a mobile environment. An individual mobile node may attempt to benefit from other nodes, but refuse to share its own resources. Such nodes are called selfish or misbehaving nodes and their behaviour is termed selfishness or misbehaviour. A selfish node may refuse to forward the data it received to save its own energy.

MANET has two types of network, namely single-hop and multi-hop [1]. In a single-hop network, all nodes within the same radio range communicate directly with each other. In a multi-hop network, nodes rely on other intermediate nodes to transmit if the destination node is out of their radio range.

A mobile ad-hoc network is a self-configuring network of mobile routers (and associated hosts) connected by wireless links - the union of which form a random topology. The routers are free to move randomly and organize themselves at random; thus, the network's wireless topology may change rapidly and unpredictably. Such a network may operate in a standalone fashion, or may be connected to the larger Internet. Minimal configuration and quick deployment make ad hoc networks suitable for emergency situations like military conflicts, emergency medical situations.

However, the open medium of MANET is vulnerable to various types of attacks. For example, due to the nodes' lack of physical protection, malicious attackers can easily capture and compromise nodes to achieve attacks. Attackers can easily insert the malicious or incorporate nodes into the network to achieve attacks. Such misbehaving nodes need to be detected so that these nodes can be avoided by well behaved nodes. Many schemes and intrusion detection systems proposed to detect such nodes.

II. TYPES OF ATTACKS IN MANET

There are many types of attacks affecting the behaviour and performance of MANET. Attacks can be classified according to its domain, protocols and means of attack.

The attacks can be classified into two types namely, outsider and insider attacks, according to the domain of the attacks. Insider attacks are carried out by the compromised nodes, which are actually part of the network. Outsider attacks are carried out by the nodes which do not belong to the network. Insider attacks are more severe than outsider attacks because insiders known secret information in the network and have privileged access rights.

The attacks can also classify into 2 major categories: active and passive attacks according to the attack means. Passive attacks obtain the data exchanged in the network without disrupting the operation, while an active attack involves interrupting the information, modification, thereby disrupting the normal functionality of MANET.

Some attacks make use of stealth to hide their action from the individual who is monitoring the system or from the intrusion detection system.

III.LITERATURE REVIEW

3.1 EAACK-A Secure Intrusion Detection System for MANET

MANET does not require a fixed network infrastructure; every single node works as both a transmitter and a receiver. Nodes communicate directly with each other when they are both within the same communication range [2]. Otherwise, they rely on their neighbors to relay messages. The self-configuring ability of nodes in MANET made it popular among critical mission applications like military use or emergency recovery.

The open medium and wide distribution of nodes make MANET vulnerable to malicious attackers. In this case, it is crucial to develop efficient intrusion-detection mechanisms to protect MANET from attacks.

In this paper it proposes a new system called EAACK-Enhanced Adaptive ACKnowledgement is specially designed for MANETs to detect the attackers. EAACK is an acknowledgement based scheme. EAACK is an acknowledgment-based IDS. This scheme makes use of digital signature. It requires all acknowledgment packets to be digitally signed.

This new system requires acknowledgement for the every packet sent to the receiver with the signature. First after sending packets to the receiver it waits for the acknowledgement. Within the predefined time interval the source received the acknowledgement from receiver then the packet transmission is successful. Otherwise the source node will switch to the secure acknowledgement mode.

In secure acknowledgement mode every consecutive three nodes work together to detect the misbehaving nodes in the route. Every third node in the group needs to give acknowledgement to the first node.

If any node fails to send acknowledgement is marked as malicious node. Then the source node switches to misbehaviour report authentication (MRA) mode.

In MRA mode, source node first searches its local knowledge base for the alternative path to the destination. Upon receiving MRA packet, destination node will searches for any received MRA is stored; if it stored then ignore the new packet and the node which sends that packet marked as malicious. Otherwise the nodes marked as malicious in the packet are removed from the route in future transmission.

This system uses the digital signatures to authenticate the acknowledgement packets. Digital signatures prevent the acknowledgement packets to be forged. The sender of the acknowledgement packet must sign the packet and after the reception of the packet receiver will verify the authenticity of the packet.

This new system reduces the packet dropping attack; it is the major security threat. In case of limited transmission power, receiver collision, false misbehavior rate EAACK is a preferred IDS than the existing approaches.

3.2 Routing Misbehavior in Mobile Adhoc Networks

Most of the routing protocols in mobile adhoc networks have limitations in transmission. So the nodes in MANET assume that other nodes always cooperate with each other to relay packets. This gives opportunities to attackers to achieve the significant impact on the network with one or two compromised nodes. To solve this problem intrusion detection system should added enhanced security level.

This paper proposed an intrusion detection system called watchdog. It aims to improve the network throughput with the presence of malicious nodes. Watchdog consists of two parts namely, watchdog and pathrater. It is responsible to detect the malicious nodes misbehaviours in the network. Watchdog system has a failure counter; it is increased while the next node fails to forward the packet.

Watchdog:

Watchdog serves as IDS for MANETs. It is responsible for detecting malicious node misbehaviours in the network by overhearing the next node's transmission. It is capable of detecting misbehaving nodes rather than links. It detects malicious misbehaviours by promiscuously listening to its next hop's transmission. If a Watchdog node overhears that its next node fails to forward the packet within a certain period of time, it increases its failure counter. Whenever a node's failure counter exceeds a predefined threshold, the Watchdog node reports it as misbehaving.

Pathrater:

Pathrater is used here as response system. It uses the feedback given by the watchdog part about the malicious misbehaviours of the node. It cooperates with routing protocol to avoid the reported malicious nodes in future transmission.

Many implementation shows that watchdog scheme is efficient. It is capable of detecting misbehaving nodes rather than links.

3.3 Video Transmission Enhancement in Presence of Misbehaving Nodes in Manets

This paper proposes a novel intrusion detection system, which is an adaptive acknowledgment scheme (AACK) with the ability to detect misbehaved nodes and avoid them in other transmissions. It is an acknowledgement based scheme which can be considered as a combination of scheme called TACK (identical to TWOACK) and an end-to-end acknowledgement scheme called ACKnowledge (ACK).

In this system source node sends out Packet 1 without any overhead except 2 b of flag indicating the packet type. All the intermediate nodes simply forward this packet. When the destination node receives Packet 1, it is required to send back an ACK acknowledgment packet to the source node along the reverse route. Within a predefined time period, if the source node receives this ACK acknowledgment packet, then the packet transmission from source node to destination node is successful. Otherwise, the source node will switch to TACK scheme by sending out a TACK packet.

Misbehaving nodes that exhibit abnormal behaviours can disrupt the network operation and affect the network availability by refusing to cooperate to route packets due to their selfish or malicious behaviour. The aim of AACK scheme is to overcome watchdog weaknesses due to collisions and limited transmission power and also to improve TWOACK scheme.

The concept of adopting a hybrid scheme in AACK greatly reduces the network overhead. The functions of such detection schemes all largely depend on the acknowledgment packets. Hence, it is crucial to guarantee that the acknowledgment packets are valid and authentic. AACK reduces the network overhead than the TWOACK scheme while maintaining the same network throughput.

3.4 Enhanced Intrusion Detection Systems for Discovering Malicious Nodes in Mobile Ad Hoc Network

In this paper a new intrusion detection system is proposed called ExWatchdog system to overcome the weakness of watchdog system. ExWatchdog is an extension of Watchdog and its function is also detecting intrusion from malicious nodes and reports this information to the response system, Routeguard. It aims to detect nodes that falsely report other nodes as misbehaving.

ExWatchdog has two parts: Watchdog and routeguard. Either in watchdog or routeguard, each node updates ratings of nodes it knows according to the information provided by any node in the network. If a node send a false report that says other nodes as misbehaving. A malicious node could partition the network by claiming that some nodes following it in the path are misbehaving. ExWatchdog detection system solve this problem.

The source node first searches a path that has no malicious node in it from the routing table. If there is not such a path available, the source then launch a Route Discovery to find a new one. After finding a path, the source sends the message using the found path. Upon receiving the message, destination node will search its own table to see if there is a match.

If there is not a matching entry in the table, it means the node is malicious and the destination node returns a message to the source confirming that the malicious node is really malicious. If there is, destination node then compares the sum field of the passing in message with the one found in the table. If the two sums equal, it means that the malicious node forwards all packets that the source sends thus it is not malicious. On the contrary, if the two sums are not equal, the node falsely report might be malicious.

Routeguard will use this information to update the rating of corresponding node. It discovers malicious nodes which can partition the network by falsely reporting other nodes as misbehaving and then proceeds to protect the network.

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.

3.5 Detecting Forged Acknowledgements in Manet

MANET suffers from the threat that it fails to detect misbehaving node when the attackers are smart enough to forge the acknowledgement packets.

In this paper, we introduce a intrusion detection scheme with digital signature algorithm to provide secure transmission against false misbehavior report and partial dropping.

This intrusion detection system assumes the link between in the network is bidirectional. Misbehaving nodes also lies in the network. It assumes misbehaving nodes are intermediate nodes; they are neither the source node nor the destination node. In routing stage they cooperate with other nodes but they drop the packets instead of forwarding to next node.

After dropping the packets the misbehaving node generate a forge acknowledgement and sent to source node in order to conceive the source node. When the source node sends out the data packet it registers the packet ID and sent time. After receiving packet destination node need to send acknowledgement packet with packet id to source. Successful reception of acknowledgement packet at source the transmission is completed and confirmed. After certain time period the source node does not receive the acknowledgement from destination it switch to secure acknowledge mode.

In this scheme, for every three consecutive nodes along the transmission route, the third node is required to send back an S-ACK packet back to the first node to confirm receiving the packet. In this system the third node is required to sign this S-ACK packet with its own digital signature. The intention of doing this is to prevent the second node from forging the S-ACK packet without forward the packet to the third node.

This is really dangerous as the malicious node can create a black-hole in the network without being detected. When the first node receives this S-ACK packet, it verifies the third node's signature with the pre-distributed public key. On the other hand, if no S-ACK packet is received within a predefined time period; the first node will report both second node and the third node as malicious. When the source node receives the malicious report, instead of trusting the report immediately and marks the nodes as malicious, it requires the source node to switch to MRA mode to confirm.

The source node switches to MRA mode by sending out an MRA packet to the destination node via a different route. If such route does not exist in the cache, the source will find a new route. For extreme conditions when there are no alternative routes from source node to the destination node, this detection system, by default, accepts the misbehaving report.

3.6 Acknowledgement Based Routing Misbehaviour Detection

In semiautonomous mobile sensor networks, since human operators may be involved in the control loop, particular improper actions may cause accidents and result in catastrophes. For such systems, this paper proposes a command filtering framework to accept or reject the human-issued commands so that undesirable executions are never performed. In the present approach, Petri nets are used to model the operated behaviors and to synthesize the command filters for supervision.

This paper proposes the 2ACK scheme that serves as an add-on technique for routing schemes to detect routing misbehaviour and to mitigate their adverse effect. It is used to detect some selfish nodes will participate in the route discovery and maintenance processes but refuse to forward data packets. 2ACK scheme send two-hop acknowledgment packets in the opposite direction of the routing path. It is a network-layer technique to detect misbehaving links rather than nodes and to mitigate their effects.

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. 2ACK transmission takes place for every set of triplets along the route. Therefore, only the first router from the source will not serve as a 2ACK packet sender. The last router just before the destination and the destination will not serve as 2ACK receivers. To reduce additional routing overhead only a fraction of the received data packets are acknowledged in the 2ACK scheme.

TWOACK detects 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. Source send data packet to receiver. Receiver generates the 2ACK packet back to sender. Retrieval of 2ACK packet within a predefined time period indicates successful transmission otherwise both destination and intermediate nodes are reported as malicious.

IV. CONCLUSION

In this paper we have done literature survey for detecting the malicious nodes misbehaviours in mobile adhoc network (MANET). This paper shows the overview of various intrusion detection systems to detect the malicious nodes and analyze the attacks in the network and provide security against those attacks in order to provide efficient packet transmission without modification, dropping and partial dropping of packets using an efficient intrusion detection system. Our proposed system first sends data packet; if it detects any misbehaviour in the network it will find the misbehaving node and eliminate the node from the route. Otherwise it will select the alternate route from its local knowledgebase and start sending packet. This system performs well in presence of false misbehaviour reports compared to other intrusion detection system and also reduce the packet dropping.

REFERENCES

[1].Elhadi M. Shakshuki, Nan Kang, and Tarek R. Sheltami, "EAACK- A Secure Intrusion Detection System for MANETs" IEEE trans. Vol.60, no.3, MAR, 2013.

[2].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.

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

[5].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

[6]. 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.

