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. 3, Issue. 8, August 2014, pg.404 – 410

SURVEY ARTICLE

A Survey on Acknowledgment-Based IDS in Mobile Ad hoc Network (MANET)

Ms. Y.Gowsika[1], Dr. R.Pugazendi[2]

[1]Department of Computer Science, K.S.Rangasamy College of Arts and Science, Tiruchengode, TamilNadu, India

[2]Department of Computer Science, K.S.Rangasamy College of Arts and Science, Tiruchengode, TamilNadu, India

[1] gowsikayogaraj@gmail.com; [2] pugazendi_r@rediffmail.com

Abstract—The progress to wireless network beginning with wired network has been a universal development model in the past years. The capability to move one place to another and adopt the infinite number of nodes brought by wireless network prepared it feasible in many applications. Between all the modern wireless networks, MANET is one of the main significant and unique applications. On the different to traditional network design, MANET does not engage a predetermined network framework; each single node works as uniformly a transmitter and a receiver. Nodes communicate straight with each other when they are both within the related communication range or else, they depend on their neighbours to broadcast the messages. The self-configuring capability of nodes in the MANET through it admired between important mission applications related to military utilize and emergency recovery. They are generally formed in the conditions of emergency and non-permanent operations or basically if there are no resources to set up involved networks. The results for traditional networks are usually not sufficient to offer efficient Ad-hoc operations. Both the infrastructure less network and disseminated nature lead the Mobile ad hoc network defenceless to malicious attackers. In this situation it is important to build up efficient intrusion detection processes to preserve MANET from attacks. Different level of security problems are raised by the wireless environment of communication and requirement of any security infrastructure. This manuscript aims of the relative learning of intrusion detection system known as Enhanced Adaptive ACKnowledgement (EAACK) especially for mobile adhoc networks. The most important aim has been situated on study of EAACK method and its restriction.

Keywords: Mobile Ad hoc Network (MANET), Intrusion Detection System (IDS), Enhanced Adaptive ACKnowledgement (EAACK) and malicious or misbehaving nodes

I. INTRODUCTION

Mobile Ad hoc NETwork (MANET) is a group of mobile nodes capable of with mutually a wireless transmitter and a receiver that communicate through each other via bidirectional wireless associates moreover directly or indirectly. The configuration process of MANET could be differing. It depends upon its application whether it is small or large. A static system is decided powerfully and it is totally controlled with the system which is large scale, mobile and highly active system. Every node is working with both transmitter and receiver. Nodes communicate straight with each other while they are both contained by the same communication range. Or else, they rely on their neighbours to communicate messages. Industrial remote access and control via wireless networks are suitable new and more admired these days. One of the most important of wireless networks is its capability to permit data communication among dissimilar parties and still keep up their mobility. Within the range of

transmitters, this communication is slightly restricted. Two nodes cannot able to communicate with each other efficiently while the distance between two nodes is outside of the communication range. By allowing intermediate nodes MANET resolves this complexity. To hand there are two kinds of MANETs: closed and open. In a closed MANET, all mobile nodes assist through each other toward a general goal, such as emergency search and law enforcement operations. In an open MANET, various mobile nodes with dissimilar goals, share their resources in order to make sure global connectivity. Various resources are consumed rapidly as the nodes participate in the functions. Battery power is measured to be more significant in a mobile environment. An individual node of a MANET comprises the benefits of other nodes but it refuses to share its own resources. Such nodes are called as misbehaving nodes or selfish nodes. A selfish node may decline to forward the data it received to save its own energy. MANET has two types of networks such as single-hop and multi-hop. All nodes communicate directly through each other which are surrounded by the same radio coverage area range. In a multi-hop network, if the destination node is out of their radio range an individual node should depend on other intermediate nodes to transmit.

A self-configuring network of mobile nodes that are attached by wireless links is typically known as MANET. The nodes can easily move and arrange randomly. The wireless topology of the network may be modified rapidly and impulsively. It may control in an unrelated fashion or associated to huge Internet resources.

However the ability of open medium of MANET is defenceless to various types of attacks. Attackers can easily insert the malicious or incorporate nodes in the network to attain attacks. Several schemes and intrusion detection systems proposed to detect such nodes.

II. RELATED WORKS

David B. Johnson et al. recommended dynamic source routing protocol for MANETs. Since in the mobile adhoc networks the mobile hosts are randomly moved [1]. Due to the restricted range of transmission one mobile node needs other mobile node to forward the data packets. Source routing is one of the routing techniques in that the sender of the packet determines the entire sequence of nodes to forward the data packets. This routing either uses static or dynamic source routes. The periodic routing ad messages are not utilized by the dynamic source routing protocol which retreating network bandwidth overhead at unimportant host movement. The mobile adhoc network has low battery power. Dynamic source routing protocol adapts to change the processes such as like host movement, however needs no routing protocol overhead.

Marti.et.al [2] proposed an IDS called watchdog. It aims to improve the network throughput with the occurrence of malicious nodes. Watchdog consists of two parts specifically, watchdog and Pathrater. It is dependable to identify the malicious node misbehaviours in the network. Watchdog system has a failure counter. It is increased even as the next node fails to forward the packet.

Watchdog: IDS are provided by Watchdog for MANETs. The process of detecting malicious node misbehaviours depends on Watchdog by listening the transmission of next node. It is accomplished of detecting misbehaving nodes rather than links. It detects malicious misbehaviour by promiscuously pay attentioning to its next hop's transmission if next node of Watchdog fails to forward the packet within a certain period of time; it increases its failure counter. The Watchdog node for MANET is said to be mischievous node if threshold value is smaller than failure counter value of watchdog node.

Pathrater: Pathrater is employ here as response system. It makes use of the feedback given by the watchdog part about the malicious misbehaviours of the node. It assists with routing protocol to avoid the reported malicious nodes in future transmission. Many implementations show that watchdog scheme is efficient. It is capable of detecting misbehaving nodes rather than links.

Yih-Chun Hu et al. proposed a novel secure on-demand ad hoc network routing protocol, called Ariadne to avoid attackers [3]. Ad hoc networks did not require predetermined network infrastructure such as base stations or access points, and can be quickly and efficiently set up as desired. Ariadne can validate the routing messages, by using any one of the three schemes. All pairs of nodes employed a shared secret key among them**.** Shared secret keys among communicating nodes shared with digital signatures**.** The requirement for harmonization IS EVADED by the pair wise shared keys and the cost of higher key setup is overhead. Ariadne also demands that each node has an authentic component of the Route Discovery chain of each node initiating Route Discoveries. These keys can be set up in the related method as a public key. This paper has offered the planning and analysis of Ariadne, a novel secure ad hoc network routing protocol. Ariadne provides security beside one compromised node and arbitrary active attackers, and depends only on efficient symmetric cryptographic operations. Ariadne functions on-demand, dynamically determining routes among nodes only as needed; the design is supported on the fundamental operation of the DSR protocol. Rather than generously concerning cryptography to an existing protocol to accomplish security, however re-designed each protocol message and its processing. The security methods we designed are highly proficient and universal, so that they should be appropriate to securing a wide variety of routing protocols. Since here doesn't secure the optimizations of DSR in Ariadne, the resulting protocol is less efficient than the highly optimized version of DSR that runs in a trusted

environment. Source routing allows the sender to avoid malicious nodes, and facilitates the sender to verify every node in a ROUTE REPLY. Such fine-grained path control is not present in most distance vector routing protocols, which makes such protocols more difficult to fully secure.

Animesh Patcha et al. proposed Collaborative Security Architecture for detecting the Black hole attack in the mobile adhoc networks [4]. Watchdog node has the ability of predicting next node whether it can send packet or not. If the next node does not able to forward the data packet into the next level then the watchdog node denotes it as misbehaviour node. If it is greater the threshold then the node is consider as malicious. But the watchdog occasionally incorrectly reports other nodes are malicious. This paper proposes a collaborative system to predict and keep out misbehavior nodes that act in groups or alone. The focus is at the network layer, using the Adhoc On-demand Distance Vector Rooting (AODV) protocol as an example.
Here demonstrates an extension to the *watchdog* approach to incorporate a collaborative system to address the collusion between nodes. In this method nodes are classified into trusted and ordinary nodes. It is assumed that when a network is formed. The first few nodes that form a network are trusted nodes. This classification of nodes into trusted nodes and ordinary nodes, and the selection of watchdogs from only trusted nodes for a given period of time, ensures that such problems of false reporting do not occur.

Sevil Şen et al. proposed IDS for the MANETs [5]. In the absence of a fixed infrastructure to offer communications MANET is a technology for some applications such that environmental monitoring, conferencing, military applications. Owing to the temporary infrastructure of the MANET security is an important concern. Consequently, with the aim of address this issue the intrusion detection system is used. Intrusion detection system has the three major mechanisms such as data detection, data collection and data response. The data collection components do the process of collecting and pre-processing. The Detection module of MANET carries out the processes like transfer the data, data storage and sending data. The detection component data is investigated for identifying the intrusion attempts**.** This work proposed two-level no overlapping Zone-Based Intrusion Detection System (ZBIDS). This method is used to fit the unique constraint of MANETs. First, in the low-level of ZBIDS, introduce an intrusion detection agent model and also proposed a Markov Chain based anomaly detection technique. Routing table related features are also called as local and trusted communication behaviours. They are designed with low processing errors which are derived from raw data. To capture the temporal dependency, a markov chain based normal profile is used. Some important network activities are supervising it and also it has the dynamic nature of raw data. A local detection model is proposed additionally to rectify the ubnormal activities. This model achieves the features such as low false positive ratio and high detection ratio. Second, proposed a non-overlapping Zone-based framework to manage locally generated alerts from a wider area. An alert data model matched to the Intrusion Detection Message Exchange Format (IDMEF) is proposed to suit the requirements of MANETs. Furthermore, an aggregation algorithm utilizing attribute similarity from alert messages is proposed to integrate security associated information from a wider area. In this manner, the gateway nodes of ZBIDS can decrease the false positive ratio; increase the detection ratio, and propose new analytical information about the attack. Third, MANET IDSs require considering mobility impact and changing their behaviour dynamically.

Liu.et.al [6] introduced the 2ACK approach that gives as an add-on method for routing schemes to detect routing misbehaviour and to mitigate their adverse effect. It is used to identify some selfish nodes will contribute in the route discovery and maintenance processes but reject to forward data packets. 2ACK approach forwards two hop acknowledgment packets in the opposite direction of the routing path. It is a network-layer method to predict misbehaving links more willingly than nodes and to moderate their effects. The 2ACK technique identifies misbehaviour through the use of a novel type of acknowledgment packet, called as 2ACK. A 2ACK packet is allocated a fixed route of two hops in the conflicting way of the data traffic route. 2ACK transmission is performed for every set of triplets along the route. Consequently, only the first router from the source will not provide as a 2ACK packet sender. The router located before the respective destination node is known as last router node and it cannot able to provide acknowledgements like 2ACK receivers. Received data packets are acknowledged to moderate supplementary routing overhead in the 2ACK approach. By acknowledging every data packet transmitted over every three successive nodes which are along with the path from the source to the destination, Malicious links are predicted by 2ACK. Recovery of a packet, availability of each node along the route are the essential tasks to give back acknowledgment packet to the node. It is located two hops away from source. Receiver receives data packet from Source. The 2ACK packet produced by receiver that sends back to sender. Both destination and intermediate nodes are referred as malicious or the recovery of 2ACK packet within a predescribed time period indicates winning transmission.

Nasser and Chen [7] proposed a novel intrusion IDS called ExWatchdog system to address the weakness of watchdog system. ExWatchdog is defined as an extension of Watchdog. The intrusion from malicious nodes is predicted by ExWatchdog and they are intimated to Route guard. Main goal of this method is to identify nodes that falsely report other nodes as misbehaving. ExWatchdog contains two main parts such as Watchdog and Route guard. In the network, either in watchdog or route guard every node update its ratings which could be based on the information offer by nodes. If a node forwards a false report then that

reports other nodes as malicious. A malicious node could divide the network by maintaining that some nodes next it in the path are misbehaving**.** The issues has addressed by ExWatchdog detection system. From the routing table the source node investigate a path with no misbehaving node. If such paths are not available means, Route discovery was beginning by the source to find new path. After finding a path, the source sends the messages to destination and the destination node checks for the match by receiving the message that send by the sender and it search for its own table. If there is not a similar entry in the table, then the node is considered as malicious node after that the destination node will send a message to the source verifying that the misbehaving node is really malicious node. If there is, destination node then evaluates the sum field of the passing in message with the one found in the table. The misbehaving node sends all packets when the two node sums are equal. If two sums are not equal, the node is said to be malicious. Route guard will use this information to update the rating of resultant node. Malicious nodes can classify the network by misbehaving and falsely reporting other nodes and let it to guard the network.
The important feature of the proposed system is its capability to determine malicious nodes which can divide the network by falsely reporting other nodes as misbehaving and then continues to guard the network.

Jin-Shyan Lee et al. proposed a command filtering framework which is used to allow or reject the human-issued commands. As a result, unwanted executions are never processed [8]. Here Mobile robots are used in peer-to-peer P2P communications instead of using client-server architecture. A command filter is used to evade the improper control actions from being passed out as the robot receives the human commands. In the course of the wireless network the human operator forwards command requests to the mobile robot. By using the distributed P2P communication the command filter obtains the system status and defines decision to accept or reject the commands in order to meet the conditions.
The function of the command filter is to cooperate with the human operator and the mobile robot in order that the closed human-in the loop system meets the necessities and assurances that disagreeable executions never occur. By using the P2P communication there is an improvement in scalability, toughness, and fault tolerance, resilience to attack and improved support and management in distributed cooperative environments. For such systems, this work introduces a command filtering framework to accept or reject the human-issued commands so that unattractive executions are never operated. In the proposed technique, Petri nets are used to model the operated behaviours and to produce the command filters for management. A collision avoidance requirement satisfies the remote commands from the human operator during the system operation.

Kang, Shakshuki and Sheltami [9] present an intrusion detection scheme with a digital signature algorithm to provide secure transmission against the false misbehaviour report and partial dropping. This new IDS assumes the link between in the network is bidirectional. Malicious nodes also lie in the network. It assumes malicious nodes are intermediate nodes. In other words, it is neither the source node nor the destination node. In routing stage they work together with other nodes. However they fall the packets in place of sending to next node. The malicious node creates a fake acknowledgement and forward to source node under its consideration, after dropping the packet. The time duration has send by the source node and it registers the packet ID when it forwards the data packet. Then the destination node required for sending acknowledgement packets with packet ID to the source. Winning reception of acknowledgement packets at the source the transmission is finished and established. After a certain time period the source node does not obtain the acknowledgement from the destination it switch to protect acknowledge mode. In order to authenticate the receiving packet, the third node wants to send back an S-ACK packet back to first node .This has to be done for every three successive node along with the transmission route. In this scheme the third node needs to sign this S-ACK packet with its own digital signature. The main objective is to avoid the second node from forging the S-ACK packet without forward the packet to the third node. This is actually risky as the malicious node can produce a black-hole in the network without being detected. After receiving the S-ACK packet by the first node, it checks the third nodes signature with the redistributed public key. Conversely, if no S-ACK packet is received within a estimated 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 report, then the node referred to as malicious and the source node needs to change as MRA mode to validate. The source node changes to MRA mode by forwarding an MRA packet to the destination node which is send through a different route. The source will determine a new route when altered route not available in a cache. For great conditions when there are no substitute routes from source node to the destination node, this detection system, by default, accepts the misbehaving report. EAACK is based on both DSA and RSA algorithm. The three important parts of the EAACK approaches are ACK, secure ACK (S-ACK), and misbehavior report authentication (MRA). An acknowledgement based IDS are referred as EAACK. This approach is used the digital signature technique to avoid the attacker. Before the acknowledgement packets forward EAACK needs the entire acknowledgement packets are digitally signed and confirmed by its receiver until they are allowed. EACK shows that high malicious behavior rates without decreasing the network performances.

ACK

ACK is principally end-to-end acknowledgement scheme. It presents as a part of the hybrid approach in EAACK, plan to decrease network overhead when no network misbehavior is predicted. In the ACK mode, the node S sends the ACK data

packet P_{ad1} to the destination node D. After sending the ACK data packet all the intermediate nodes between the source and destination are mutual and node D successfully receives P_{ad1} packet it requires to send the ACK packet P_{ak1} back to the node S with same route but in reverse order. The data transmission gets successful when the node S receives the packet. Besides, the malicious nodes are identified when the node S will convert to S-ACK mode by forwarding an S-ACK data packet.

S-ACK

In the S-ACK scheme to detect the misbehaving nodes every three successive nodes work in a group. From these three successive nodes, the S-ACK acknowledgement packet received by first node from third node.
The S-ACK method is able to identify the malicious nodes even with receiver collision and low transmission power. In the S-ACK scheme the three successive nodes F1, F2, and F3 work as a collection to detect the malicious nodes. At first node F1 sends the S-ACK packet P_{sad1} to node F2. Then the node F2 forwards to node F3. The node F3 has a response to send back acknowledgement packet S-ACK P_{sak1} packets to node F2, after it receives the P_{sad1} packet. Node F2 sends P_{sak1} to F1. Within a threshold time the node F2 and F3 are referred as misbehaviour nodes and the node N1 does not obtain the acknowledgement packet. Finally the S-ACK can be reported by F1 node and it inform to the source node.

MRA

Actually in the watchdog it fails to identify the misbehaving nodes due to the presence of false misbehavior report. Since of this fake result information the watchdog consider normal nodes as malicious nodes. To overcome this difficulty, the MRA method is to validate whether the destination node has received the result missing packet via a different route. For this the source node fetches its local data and identifies the route to the destination node. The alternate route is found by using DSR routing request when there is no route to destination. Local data are compared with the MRA packet that is received by the destination node. The result considered as a fake misbehaviour report when MRA packet receives earlier.

DIGITAL SIGNATURE

The acknowledgement based detection systems that based on EAACK are ACK, S-ACK and MRA. The three schemes rely on acknowledgment packets to detect the misbehaviors in the network. All acknowledgement packets in the EAACK are reliable and pure. Or else the attackers forge the acknowledgement packets; all the three schemes are susceptible. So, here include digital signature in EAACK to make certain the reliability of IDS. All the acknowledgment packets are to be digitally signed before they are forward and set until they are accepted. But it needs additional resources owing to the digital signature in MANETs. To overcome this here DSA and RSA digital signature schemes are used in MANETs.

TABLE I
ANALYSIS OF METHODS

S.No	TITLE	AUTHOR	METHODS	ADVANTAGES	DISADVANTAGES
1	Dynamic Source Routing in *ad hoc* wireless networks [1]	D. Johnson and D. Maltz	Dynamic Source Routing	Overhead of the protocol is quite low, protocol performs well	Does not address the security concerns inherent in wireless network or packet routing
2	Mitigating routing misbehavior in mobile ad hoc networks [2]	S. Marti, T. J. Giuli, K. Lai, and M. Baker	Watchdog and Pathrater	Increase the throughput.	Increasing the overhead transmissions.
3	ARIADNE: A secure on-demand routing protocol for ad hoc networks [3]	Y. Hu, A. Perrig, and D. Johnson	Ariadne	Prevents many types of Denial-of-Service attacks.	Did not secure the optimizations of DSR in Ariadne.
4	Collaborative security architecture for black hole attack	A. Patcha and A. Mishra	collaborative architecture	Tackle collusion amongst nodes.	Increases the network overhead.

	prevention in mobile ad hoc networks [4]				
5	Intrusion detection in mobile ad hoc networks [5]	B. Sun	Zone-Based Intrusion Detection System (ZBIDS)	Achieve low false positive ratio and high detection ratio.	Doesn't to analyze and categorize MANET attack models and system vulnerabilities.
6	An acknowledgment-based approach for the detection of routing misbehaviour in MANETs [6]	K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan	2ACK scheme	Reduce extra routing overhead, does not suffer from transmission power problem.	Computational complexity and time complexity of the system is high.
7	Enhanced intrusion detection systems for discovering malicious nodes in mobile adhoc network [7]	N. Nasser and Y. Chen	ExWatchdog	Decrease the overhead greatly, solves a fatal problem	Does not increase the throughput, falsely report
8	A Petri net design of command filters for semiautonomous mobile sensor networks [8]	J.-S. Lee	command filter for semiautonomous MSNs	Very compact model, high feasibility	Limitations for structured environments
9	Detecting misbehaving nodes in MANETs [9]	N. Kang, E. Shakshuki, and T. Sheltami	EAACK (Enhanced Adaptive ACKnowledgement)	Higher malicious behavior detection rates, positive performances in various test scenarios	It suffers from extra amount of network overhead

III. CONCLUSION

This detailed literature survey has been conducted for various Intrusion detection system in MANET. This work introduces the general idea of various intrusion detection systems to discover the malicious nodes and to analyze the attacks in the network. It offers security against those attacks in order to provide efficient packet transmission as the same, partial dropping of packets and deleting using an efficient intrusion detection system. The approach mentioned above are dynamic source routing protocol, Watchdog, TWOACK, and Adaptive ACKnowledgment (AACK), Ariadne, Zone-Based Intrusion Detection System, ExWatchdog, S-ACK and EAACK has been discussed. Each of the above surveyed methods demonstrates and shows better in some extent and not in entire categories.

REFERENCES

[1]. D. Johnson and D. Maltz, "Dynamic Source Routing in ad hoc wireless networks," Series title: The Kluwer International Series in Engineering and Computer Science, ISBN: 978-0-585-29603-6, vol.353, ch. 5, 1996, pp. 153–181.

[2]. 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, USA, from Aug. 06 to Aug. 11, 2000.

[3]. Y. Hu, A. Perrig, and D. Johnson, "ARIADNE: A secure on-demand routing protocol for ad hoc networks," in Proc. 8th ACM Int. Conf. MobiCom, Atlanta, USA, from Sep. 23 to Sep. 28, 2002.

[4]. A. Patcha and A. Mishra, "Collaborative security architecture for black hole attack prevention in mobile ad hoc networks," In Proc. Radio Wireless Conf., from Aug. 10 to Aug. 13, 2003.

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

[6]. K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An acknowledgment-based approach for the detection of routing Misbehaviour in MANETs," IEEE Trans. Mobile Comput., ISSN: 1536-1233, vol. 6, no. 5, May 2007, pp. 536–550.
[7]. N. Nasser and Y. Chen, "Enhanced intrusion detection systems for discovering malicious nodes in mobile adhoc network," In Proc. IEEE Int. Conf. Commun., Glasgow, Scotland, from Jun. 24 to Jun. 28, 2007.
[8]. J.-S. Lee, "A Petri net design of command filters for semiautonomous mobile sensor networks," IEEE Trans. Ind. Electron., ISSN: 0278-00486, vol. 55, no. 4, Apr. 2008, pp. 1835–1841.
[9]. N. Kang, E. Shakshuki, and T. Sheltami, "Detecting misbehaving nodes in MANETs," in Proc. 12th Int. Conf. iiWAS, Paris, France, from Nov. 8 to Nov. 10, 2010

