International Journal on Future Revolution in Computer Science & Communication Engineering
Volume: 2 Issue: 11
ISSN: 2454-4248
12 – 18

A Survey on Intrusion Detection System in MANET

Bhagyashali Kokode, Prof. Mukul Pande, Prof. Sarvesh V. Warjurkar

Abstract: A mobile ad hoc network is an infrastructure less network which is prone to various malicious attacks when incorporated in applications. It is a dreadful task for attaining security to the greatest degree in MANET. This is awaited to the diverse characteristics of mobile ad hoc networks which unlike from well-established infrastructure network. In order to overcome this security challenges the Intrusion detection systems have been deployed in the ad hoc network. In this paper we focus on surveying heterogeneous intrusion detection systems used in MANET for defending various attacks.

Keywords— *Mobile Ad hoc Network; IDS; Routing protocols; Attacks*

*****

I. INTRODUCTION

A mobile ad hoc network is diverse from infrastructure network and lack of firm base stations. MANET altogether utilized in various emergency applications, Mobile Ad hoc Networks (MANETs) present most significant merits and have been incorporated in a varied range of applications such as disaster assistance [17], monitoring of environment [18] and vehicular networks [19].Mobile ad hoc network also includes the wide space of vulnerabilities due to their challenges, which impacts the degradation of the network, hence assured communication in mobile ad hoc network is difficult.

Challenges in mobile ad hoc network includes the absence of reliability in-between nodes due to its mobility and changing topology rapidly, hence it is more prone to malicious attacks. Lack of security in network which leads the intruder to interrupt the transmission of data which leads towards data loss. Insufficiency in the quality of service due to rapid change of topology. Energy Consumption drastically affects the data transmission between the mobile nodes.

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 and encryption would be used as the primary defense. Nevertheless those techniques lacks the well-organized defense to the attack[26],hence to overwhelm this attacks and challenges in MANET intrusion detection systems have been deployed in ad hoc network.

An efficient way to detect an attack that occurs in a MANET is the incorporation of an Intrusion Detection System (IDS) [1]. An IDS [20] is a software that 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 nodes. In fixed networks, intrusion detection and system (IDS) acts as a second layer of defense beyond a firewall; whereas in MANETs IDS becomes the front line of defense to protect nodes from attackers [5] [24].

Unlike the fixed infrastructure the mobile ad hoc network lacks the access point and routers hence the IDS is deployed in each nodes of the ad hoc network due to the lack of centralized control. Many existing intrusion detection algorithm don't indulge in punishment which makes the intruder nodes behavior normal, in order to overcome those demerits many novel intrusion detection system algorithm proposed. This paper discusses the survey of the Previous intrusion detection algorithms and their approach towards the malicious attacks caused due to its infrastructure less and dynamic nature. In order to defend those attacks various intrusion detection system algorithms have been deployed in various mobile ad hoc nodes to overwhelm the malicious attacks.

The IDS algorithm tends to detect the malicious attack and isolate the nodes and also the comparison and suggested work of those algorithm presented The rest of the paper is ordered as, Section 2 depicts the background of mobile ad hoc networks and the intrusion detection system, section 3 comprises the survey of previous work which incorporates IDS in MANET, comparison of algorithm, section 4 comprises the conclusion.

This section presents the basic information about MANET, Routing Protocols, Types of Attacks and IDS that are required for the proposed work.

A. MANET

A mobile ad hoc network is a self- assembling system of mobile nodes that communicate with each other through wireless links without fixed infrastructure.

MANET comprises the characteristics of mobility of nodes, vulnerability of nodes which leads capturing of nodes by attacker, frequently changing topology, More energy consumption, lack of security, so it is prone to variety of attacks such as routing, packet modifications, eavesdropping

and protecting a MANET under such environments is difficult. MANET have no access points to transfer data towards nodes, it is done through multiple hops. Mobile node exhibits itself as both host and router to create a route.

B. ***Routing Protocols***

MANETs routing protocols classified as either proactive or reactive. Proactive routing protocols were FSR, OSLR whereas reactive protocols includes AODV, DSR, etc. Proactive protocol not much productive as reactive protocols because of their overhead hence reactive routing protocols such as AODV and DSR mostly used in MANETs. In a proactive routing protocol [10] each node proactively looks for routes to further nodes, which regularly interchange routing messages, in order to maintain routing table up-to-date and error-free., the node will be maintaining one or more tables to save the information of the routes used for transmission of packets .

Due to limited constraints of energy consumption and bandwidth of MANET nodes, periodic transmission of routing messages would lead to the congestion of the network. In a reactive routing protocol [10] a route is analyzed and formed when two nodes decides to forward the data, if the source needs the route to a destination it will establish a route by route discovery procedure.

C. ***Types of Attacks***

Identical to other wireless networks, ad hoc networks are prone to passive and active attacks , Passive attacks leads to eavesdropping of data, whereas active attacks contains actions accomplished by intruders such as replication, modification and deletion of exchanged data . We can also categorize MANET attacks into three such as routing, multipart and performance [2]. Routing attacks constitutes Black hole attack, Wormhole attack, Packet Modification, multipart attacks consist of Neighbor attack, performance attacks constitutes DoS attacks, Sleep deprivation.

Black Hole Attack

It is the kind of attack where the intruder first needs to invade into the nodes and then drops some or all data packets. Rather transmitting the packets further along the path .The impact of this leads to poor dispatch of packet ratio. Algorithm [12] two in section 3.

A proposes the MDSR scheme which makes the malicious node to be isolated and thus obtaining the normal behavior.

Wormhole Attack

It is the one where the attacker documents the packets from one place and tunnel them to another place in the ad hoc networks, those packets are returned back into the network. Algorithm 1[15] in section 3.A proposes the antiworm hole mechanism for prevention of worm hole attacks in mobile ad hoc network routing

Gray Hole

Gray hole too is a part of denial of service attack [25]. Gray hole attack is an add- on to black hole attack. Gray whole attacks makes the intruder node to broadcast the similar action as a genuine node during discovery of route, which leads to dropping of packets from particular nodes. It is a major concern since it is difficult to identify this attack. Algorithm[4][5][6] in section 3.A provides the solution for detecting gray hole attack and isolate those intruder nodes.

Rushing Attack

It uses forged suppression during the route discovery process are prone to this attack. An attacker which could transmit further route request rapidly than genuine nodes can enlarge the chance that the routes include the attacker will be found instead of authentic route[21],rushing attack prevention provides the defensive process against the attack.

Sleep Deprivation (SD)

It is a denial of service [8]attack in which an attacker interacts with the node in a manner that appears to be legitimate, but where the purpose of interaction is to keep the victim node out of its power conserving sleep mode. Algorithm [4] [5] [6] in section 3.A provides the solution to overwhelm the attacks.

Sybil Attack

Each node in a mobile ad hoc networks seeks a significant address to participate in routing, and nodes are identified through this address in the network [23]. There is no central authority to verify these identities in MANETs. An attacker can exploit this property and send control packet, for example RREQ or RREP, using different identities this is known as a Sybil attack [23].Algorithm[4][5][6] in section 3.A provides the solution to overwhelm the attacks.

D. IDS

The Intrusion detection system is a method for detecting the attacks by analyzing and continuously monitoring network functions. Intrusion detection arises as a crucial defensive mechanism in mobile ad hoc networks. Intrusion detection systems would be deployed in each mobile node to monitor local traffic and to detect occurrence of local intrusions. These nodes can forward the intrusion information to neighbors when needed. Another technique in the IDS is to deploy intrusion detection system for self and neighbor nodes to check for malicious neighbor nodes present. The global intrusion detection system can be deployed for clusters of mobile nodes where cluster head node is responsible for global intrusion detection for its cluster

 ISSN: 2454-4248
12 – 18

[3].Three significant components of IDS include data collection, detection, and response [4]. The data collection is responsible for transferring data to a common format, data storage and sending data to the detection module [4].

The intrusion detection system gathers the audit data and cross check the data in order to find any attack in the network, with the established data usedfor auditing the IDS could be classified ad host and network based [22].A network based generally present in the gateway of the network and examines the packet whereas the host based system uses the operating system data to examine the attacks in the network. IDS classifications is of various types primarily includes Active and passive IDS, The active attack is set for automatic blocking of suspecting attacks which provides real-time remedial action for respective detecting attacks. A passive IDS is a system which is deployed to for monitoring and analyzing network traffic activity and provide caution to the nodes regarding vulnerabilities and attacks.

A knowledge-based Intrusion Detection Systems which consists of the database of previous attacks signatures and known system vulnerabilities for taking responsive actions. Anomaly-based Intrusion Detection Systems is the process of collecting data related to the performance of authorized nodes over a span of time which followed by examination applied to noticed behavior to determine with a highest degree of confidence that the behavior of intruder nodes not authorized. Even though false alarm rates is a primary problem for developing the intrusion detection system especially the anomaly based intrusion detection system, yet the system has fully met the desired objectives compared to the signature based system[9].Specificationbased intrusion detection which frames specifications that capture authorized nodes behavior any variation from the framed specification marked as an attack.

II. RELATED WORK

Various IDS algorithms related to our work have been discussed with their merits and demerits.

A. Various IDS Algorithm

Algorithm 1 - Intrusion Detection Nodes: Prevention of Wormhole Attacks in Mobile Ad Hoc Networks

In this algorithm the protective process called anti wormhole mechanism executed on an IDS node hence it sniffs routing messages of regular nodes within their transmission range executing an intrusion detection system into a MANET so as to detect and isolate wormhole nodes. Intrusion detection system nodes can find if there is a tunnel ingress node according to the pairing of RREQ and RREP in the routing protocol, and also find if there is a tunnel egress node, according to RREP, being generally processed in a justified time. If the value passes the threshold value, Intrusion detection system nodes can broadcast a block message to all hence isolating the malicious nodes that provokes wormhole attacks, Anti Worm hole Mechanism algorithm executed on all IDS nodes comprises of four steps [15], Intrusion detection system sniffing an route request to update the Request Table which maintains routes, hop count and expiration time.

It also sniffs an RREP to update the Reply Table and find the tunnel ingress wormhole node. The IDS also periodically checking the Reply table to find the tunnel egress wormhole node. The last step which includes in mechanism is that the Intrusion detection system is used to communicate between the IDSs, mainly to process the block message

Merits:

- The packet loss rate tremendously reduced hence isolating the worm hole nodes
- It prevents degradation in the performance of the packet transmission

Demerits:

- IDS nodes can rapidly block a malicious node, without false positives, If a proper threshold value is not set the intruder nodes won't be effectively isolated [15]

Algorithm 2 -Modified DSR protocol: Detection and Removal of selective black hole attack in MANET [12].

The MDSR algorithm comprises three steps [12],The source node forwards the block of packet to the destination nodes once the packet reach the destination the probability of data reached is calculated if its value is greater than threshold value of packet loss then it initiates the gray hole detection procedure. The destination node begins the detection of the presence of malicious attacks in the source route using query request and mark it as suspicious nodes.

The IDS nodes that are adjacent to the suspected nodes turn into promiscuous mode and hear whether the data packets are forwarded or dropped by the suspected nodes, if there is drop of packets then the node is isolated and the broadcast message send to all normal behavior nodes thus preventing the further attack. *Merits:*

- The IDS nodes would be swift into promiscuous mode hearing in the presence of intruding nodes results in lesser power consumption

Demerits:

- Many assumptions in the proposed work which is not applicable in real time environments such as all nodes can be similar in their physical properties such as transmission range, all nodes were authorized[12]

Algorithm 3 - DOS Attack prevention: Adaptive intrusion detection and prevention

Assess control chart, a tool used in statistical process control (SPC) used for detecting DOS which produces low detection and high false alarm rates [7]. In order to overpower those

 ISSN: 2454-4248
12 – 18

demerits they implemented adaptive intrusion detection and prevention (AIDP) mechanism, Initially uses chi-square test as an Anomaly based intrusion detection mechanism to examine the overall behavior of the network and then uses control chart for identifying intruder nodes. Finally isolates the intruder nodes.

Merits:

- AIDP exhibits a high success rate and very low false alarm rate with an affordable processing overhead on the network over a range of scenarios tested.

Demerits:

- Misused based intrusion detection (MBID) is not used, AIDP is more prone to generate false positives than MBID and also a reasonable processing overhead on the network [6].

Algorithm 4 - MANET security: Generalized intrusion detection and prevention [13].

Generalized Intrusion Detection and Prevention (GIDP) is an extension to Adaptive intrusion detection and prevention hence the combined technique of anomaly based and knowledge based intrusion detection [6] is the one which takes advantage of both techniques. Primary step include gathering data in the form of two matrices ,network characteristic matrix and a derived matrix where NCM includes details of network routing protocol whereas the derived matrix includes parameters that shows network performance. Secondary step comprises the testing phase it examines the malicious behavior in the network .If there is no intrusion then the initial training profile is updated, otherwise the cluster head detects the attack using the knowledge base information. In the event of familiar attacks cluster head discovers the malicious nodes using intruder detection constraints particular to the well-known attack.

Testing sliding window is maintained in order to detect the attack within particular time period when this threshold period exceeds then the cluster head will blacklist the node and isolated .The Generalized intrusion detection and prevention system consists of more false positives which leads to downside of security aspects in the proposed work[13]

Merits:

- It prevents diverse categories of attacks but it also has the potential to detect new attacks and the intrusive activities which provokes performance degradation

Demerits:

- Deployment of GIDP in variety of network environment is difficult, inflexibility towards the identification of attacks in the diverse environment

Algorithm 5 -Intrusion detection and prevention system: Various MANET attacks.

The proposed approach works as follows, [14]. The Cluster head continuously gathers NCM and DM parameters and formulates the initial training profiles. In the testing phase the Cluster head applies the testing module after each Time interval. The testing phase consists of several tasks, which would initially detects intrusion in the network if there is no intrusion then it updates the Initial training profile.

In case there is presence of intrusion Clustered identifies the attack using existing information in the knowledge base, if there is presence of known attacks the Cluster recognizes the malicious node and isolate. Attack identification traces the attack which does not match the rules for known attacks then the Cluster head applies the attack inferences and add that attack rules to the knowledge database.

Merits:

- Blocks the vast forms of attacks in MANETS but also has the potential to identify new unpredicted attacks.

Demerits:

- The results shows that in some cases isolating the attacker can cause more harm than good to network, hence an adaptive flexible intrusion response mechanism is required.
- More false positives produced by the detection which leads to consumption of more time and energy in MANETS [14].

Algorithm 6 -An Intrusion detection and adaptive response mechanism for MANETs

Intrusion detection and adaptive response mechanism which is the extension of work [14] which similarly uses a combinationof both anomaly-based and knowledge-based Intrusion detection. The Cluster head collects the Network characteristic and derived matrix parameters and formulates the initial training profiles In Adaptive intrusion response scheme testing operates in four phases. Intrusion detection, Attack identification Intruder Identification, Adaptive intrusion response.

The mobile node calculates the confidence level of the attack and then evaluates the network performance degradation. Finally adaptive response action is taken and the selection of the response, based on the decision table which includes varied actions such as route around attack, isolation and no punishment

Merits:

- Recognize the attacks and applies varied responsive actions based on the level of which overcomes network degradation.

Demerits:

- The proposed approach uses reactive intrusion detection approach since the attacks cannot be prevented
- Intrusion response cost is high due to energy and time consumption[11]

 ISSN: 2454-4248
12 – 18

Algorithm 7 - Security based intrusion detection scheme: Enhanced Adaptive Acknowledgment [16].

Routing protocols have many downsides hence the intruders can compromise the node and launch the attack. In order to overcome those intruding attacks the enhanced adaptive acknowledgement scheme been implemented in which acknowledged packets were used to check successful transmission of packet from source to destination. But even the acknowledgment packet could be forged by inducing the nodes, hence the digital signature is acquired which makes the acknowledged packets free from intruders, Acknowledgement scheme constitutes the primary process in which the source sends the ACK packets to the destination, if the intermediaryand source nodes were cordial then the packets will be transmitted successfully to the destination, once the packet reaches the destination node within threshold time then it sends back the ACK packet to the source node via the back order.

In case of failure of ACK scheme the secure acknowledgment(S-ACK) is used in each successive of three nodes the third nodes sends an S-ACK packet to the first node. If the first node doesn't receive those packets then it is termed as intruder nodes and generates misbehavior report which is dispatched to the source node. Due to adaptable nature of Misbehavior Report Authentication (MRA) the scheme is capable of finding intruder nodes even in the presence of fake misbehavior information

Merits:

- It overcomes the network degradation issues such as recipient crash, Battery power consumption, and Fake misbehavior information.

Demerits:

- More Network Overhead occurs due to the usage of numerous acknowledgement packets in each nodes of the network, Fragmentary packet transmission is rather possible in the network[16]

B. Parameters Considered

The Comparative analysis of previous proposed algorithms [6] [11] [12] [13] [14] [15] [16] have been described in Table 1, comprises the algorithm proposed, parameters used for the attack detection and response mechanism.

Many techniques to detect the malicious attack in mobile ad hoc network, in the survey work it uses anomaly, knowledge, control chart based process used to detect the attack. Parameters such as threshold is used hence the range is set if the calculated value passes it then the node is mapped as malicious. Responsive actions taken based on the detection of attacks, adaptive and generalized isolation is taken for denial of service, black hole, gray hole, sleep deprivation, and Sybil attacks. Digital signature based acknowledgement is used in the algorithm in order to overwhelm the forging and packet dropping.

Security is the prior concern in mobile ad hoc networks due to its dynamic characteristics hence the algorithms have been proposed to ensure the secure transmission of packets during routing. Overhead includes the usage of memory space, bandwidth, amount of resource utilized, so the overhead should be taken into primary consideration in order to make the network reliable in packet transmission. Routing protocols also taken into consideration for comparing the surveyed algorithm in order to gain significant features of them.

Table of Comparison

Existing Algorithm		**Comparison Slots**			
	Technique used	**Attack Lookup**	**Response**	**Routing protocol**	**Overhead**
Anti-worm hole Mechanism	Threshold	Wormhole	Isolation	WAODV,TAODV, MAODV,	yes
Modified DSR protocol	Threshold	Black hole	Isolation	MDSR	yes
Adaptive intrusion detection and prevention	Control chart, Anomaly	Denial of service	Adaptive Isolation	AODV,DSR	yes

 ISSN: 2454-4248
12 – 18

Generalized Intrusion detection and prevention	Anomaly and knowledge technique	Sleep deprivation, Black hole, grey hole,	Isolation	AODV	yes
Intrusion detection and prevention system: Various MANET attacks.	Anomaly and knowledge technique	Sleep deprivation, Black hole, grey hole, Rushing attack, Sybil attack	Isolation	AODV	yes
Security based intrusion detection scheme: Enhanced Adaptive Acknowledgment	Digital signature acknowledgement, Threshold	Forging, Packet Dropping	Retransmission secure Acknowledgment, Misbehavior report authentication	DSR	yes
An Intrusion detection and adaptive response mechanism for MANETs	Confidence on attack, Anomaly and knowledge technique, decision table	Sleep deprivation, Black hole, grey hole, Rushing attack, Sybil attack	Route around attack, Isolation, No Punishment	AODV	yes

III. CONCLUSION

The latest year's security in mobile ad hoc network is the demanding task. Mobile ad hoc network is an infrastructure less network which is prone to various malicious attacks when incorporated into applications, it also includes the wide space of vulnerabilities due to their challenges. In order to prevent the attack, authentication and encryption would be used as the primary defense. Nevertheless those techniques lacks the well-organized defense to the attack.

Due to this significant reason the intrusion detection system had been established which is used to defend those attacks, various intrusion detection system algorithms have been proposed and been deployed in various mobile ad hoc nodes to overwhelm the malicious attacks .In this paper the characteristics of MANET , background of mobile ad hoc network its routing protocol and various attacks created due to routing, intrusion detection system and its deployment in the mobile node is discussed , comparison of previous algorithms had been made and suggested work for future proposed system been discussed. Existing algorithms tends to detect attacks in MANET but more work required to enhance security in MANET, hence more intrusion detection algorithm should be proposed.

REFERENCES

[1] Christofis's Panos1, Christos Xenakis2, Giannis Stavrakakis1,2010 A novel intrusion detection system for MANETS International Conference on Security and Cryptography

[2] Amira, E., Anshar, E., Nazi, H.R., and Adakai, M., 2012 Survey on network access control technology in MANETs, Malacca: IEEE.

[3] Nish Dang & Poona Mitta, 2012 Cluster based intrusion detection system for MANETS, International Journal of Computer Applications & Information Technology.

[4] Sen, S., & Clark, J.A., 2008, Intrusion Detection in Mobile Ad Hoc Networks, Guide to Wireless Ad Hoc Networks, Springer.

[5] Huawei LiDas, A.Jianying Zhou, 2005,Theoretical Basis for Intrusion Detection, IEEE Proc, Information Assurance and Security.

[6] A.Nadeem and M.Howarth, 2008,―Adaptive intrusion detection and prevention of Denial of Service attacks in MANETs‖,Proceeding of ACM 5th International Wireless Communication and Mobile Computing Conference

[7] R. H. Akbani, S. Patel and D. C. Jinwala, 2012**,** DoS attacks in mobile ad hoc networks: A survey**,** in Proc. 2nd Int. Meeting ACCT.

[8] M.Pirrete and R.Brooks, 2006, ―The Sleep Deprivation Attack in Sensor Networks: Analysis and Methods of Defense‖, International Journal of Distributed Sensor networks.

[9] Garuba, M., Liu, C. &Fraites, D., 2008, Intrusion Techniques: Comparative Study of Network Intrusion Detection Systems. In Proceeding of Fifth International Conference on Information Technology: New Generation, IEEE.

[10] M. Abolhasan, T. Wysocki, and E. Dutkiewicz,2004, ―A review of routing protocols for mobile ad hoc networks,‖ Elsevier Journal of Ad Hoc Networks, 1–22.

[11] A. Nadeem, M. Howarth, 2014, An intrusion detection & adaptive response mechanism for MANETs, Elsevier Journal of Ad Hoc Networks, 368-380

[12] M. Mohanapriya, Ilango Krishnamurthy, ―Modified DSR Protocol for Detection and Removal of Selective Black Hole Attack in MANET‖, Computers and Electrical Engineering, Elsevier science, 2013

[13] Nadeem, A., &Howarth, M. (2009). A generalized intrusion detection & prevention mechanism for securing MANETs. In Proceedings of IEEE international conference on ultra-modern telecommunications & workshops, St. Petersburg, Russia.

[14] A. Nadeem, M. Howarth, 2013, A. Nadeem, M. Howarth, Protection of MANETs from a range of attacks using an intrusion detection and prevention system, Telecommunications Systems Journal Springer

[15] Ming-Yang Su , Kun-Lin Chiang,2010,Prevention of Wormhole Attacks in Mobile Ad Hoc Networks by Intrusion Detection Nodes, volume 6221 of Lecture Notes in Computer Science, page 253-260. Springer

[16] Elhadi, M. Shakshuki., Nan Kang, Tarek R. Sheltami,2013, **"**Eaack—a secure intrusion-detection system for manets**"**.ieee transactions on industrial electronics, vol. 60, no. 3 march 2013 1089.

[17] H.C. Jang, Y.N. Lien, T.C. Tsai, Rescue information system for earthquake disasters based on manet emergency communication platform, in: Proceedings of the 2009 International Conference on Wireless Communications and Mobile Computing: Connecting the
World Wirelessly, ACM, 2009, pp. 623–627

[18] A. Vasiliou, A.A. Economides, MANETs for environmental monitoring, 2006,in: IEEE International Telecommunications Symposium, , pp. 813–818.

[19] B.C. Seet, G. Liu, B.S. Lee, C.H. Foh, K.J. Wong, K.K. Lee, ASTAR: a mobile ad hoc routing strategy for metropolis vehicular communications, in: NETWORKING 2004. Networking
Technologies, Services, and Protocols; Performance of Computer and Communication Networks; Mobile and Wireless Communications, Springer, 2004, pp. 989–999.

[20] Zhang, Y., & Lee, W. 2000. **"**Intrusion detection in wireless ad hoc networks‖. In Proceeding of 6th ACM MOBICOM.