Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 3, 2021, Pages. 2444 - 2452
Received 16 February 2021; Accepted 08 March 2021.

A Study on Discovering Malicious Nodes on MANET through Secure Intrusion Detection

A.Suganya[1],S.ManojKumar[2],A.G.Vigneshwari[3]
[1] Assistant Professor,Department of Information Technology,Karpagam College of Engineering, Coimbatore
[2]Professor,Department of Information Technology,Karpagam College of Engineering, Coimbatore,
[3]Assistant Professor,Department of Computer Science[3],P.K.R. Arts College for Women, Gobichettipalayam
suganya.a@kce.ac.in

ABSTRACT: The transition from wired network to wireless network has created a tremendous technological boon worldwide. Mobile Ad hoc Network (MANET) is one among the applications of wireless network. This MANET does not require any access point for communication and hence is called infrastructure less connection. MANET haswide range of applications in critical areas like military, etc.The technology grows, it posses both pros and cons. If the communication between the nodes is considered as an advantage, then security in the communication is still a drawback. MANET is prone to several attacks by malicious nodes because of its wide distribution and wireless medium. Hence developing an efficient intrusion detection system is mandatory for protecting the MANET from the malicious attackers. But the prevention mechanism is not sufficient to ensure the security. It should be focused from the part before an attacker can attack and damage the system. Hence an efficient and prominent intrusion detection system is required to achieve the better security in MANET. This paper might help in surveying various intrusion detection mechanisms available. In this paper we aim to explore intrusion detection system for securing MANET, compare various intrusion detection system mechanisms.
Keywords: Network, Wireless communication, MANET, Intrusion Detection System.

INTRODUCTION

World is experiencing a rapid growth in computers and technology. Network plays a major role in exchanging data between two users. The requirement of fixed point infrastructure was decreased as MANET emerged. MANET stands for Mobile Ad hoc NETworks. This introduced the communication or information exchange between two mobile users who are connected in wireless. MANET has become one of the significant technologies that work without an access point. This arrangement is called infrastructure less. This property of MANET attracted many applications which are very crucial. Few such applications are military, rescue operations, education, virtual conferencing etc. Each device connected in MANET has a transmitter, receiver which helps to communicate to the next device which has its own transmitter and receiver. The MANET has mobility as a main characteristic. It never bothers the communication range of two devices which is involved in communication. This is attained by dividing the MANET into two. They are single hop network and multi hop

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 3, 2021, Pages. 2444 - 2452
Received 16 February 2021; Accepted 08 March 2021.

network. If all the nodes or users communicate directly within a same range, then it falls under single hop network. On the other side, if they lie in different range and rely on intermediate devices for communication, then it is multi hop network.

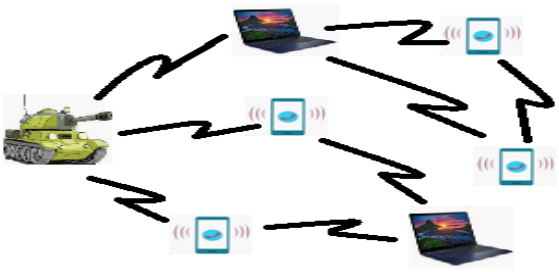

Fig 1 Mobile Ad hoc NETworks

The MANET is prone to attacks because of two reasons. First, it is wireless. Tracking anonymous users or attacks is difficult. Second, MANET is an open medium and hence anybody can join the network which cannot be restricted. Hence to ensure security, we need a mechanism to identify the attacks. But even after identifying the attacks after their occurrence, it is good if it is detected before attacking. One such detection mechanism is Intrusion Detection System (IDS). IDS is a method helping to identify unauthorized activity or un approved access to a network. IDS in MANET include two concepts Intrusion detection technique and intrusion detection architecture.

Intrusion detection system

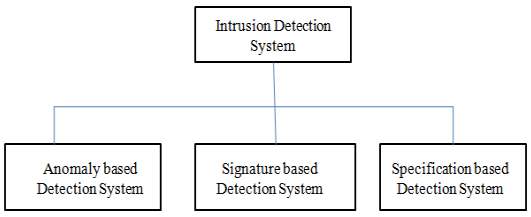

Fig 2: Taxonomy of Intrusion detection System

There are two important models available in IDS. They are signature based approaches and anomaly based approaches. A third approach called specification based detection prevails common now a day. Signature based approach follows a traditional approach. It matches the attacks with known attacks. If a new attack happens, signature based approach may fail to detect. Hence anomaly based approach is used for detecting unknown attacks in MANET. The normal behaviour of the system is captured in a trained system. If there is any deviation in the characteristic of the system that does not match the existing characteristic of a system then the misbehaving system is targeted as malicious device. In specification based detection, only specific characteristics which creates security inconvenience is targeted. If those features are irregular in behaviour with respect to the normal node, then those nodes are identified as malicious nodes.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 3, 2021, Pages. 2444 - 2452
Received 16 February 2021; Accepted 08 March 2021.

The network is divided into seven layers in the OSI model. But in general, network can be categorized into five layers. They are

1. Application layer
2. Transport layer
3. Network layer
4. Data link layer
5. Physical layer

Similar to the intrusion detection system, Intrusion prevention system also prevails. Both commonly named as Intrusion Detection and Prevention system. The IDPS gives a crystal clear view in configuration of network, execution of a network, designing and securing the network. The taxonomy of Intrusion Detection and Prevention system (IDPS) is given below.

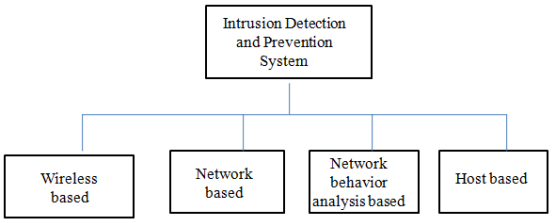

Fig 3: Taxonomy of IDPS

There are many methods or algorithms available for ensuring secured Intrusion Detection System where only popular techniques are discussed here.

LITERATURE SURVEY

Ankita Sharma et al proposed a policy enforcement technique for intrusion detection system[1]. Policy referred to rules or usage parameters which require accessing for users and authorizing them. They also addressed various attacks available in MANET such as black hole, grey hole, DoS attack etc., Ehsan Amiri et al discussed intrusion detection system and the attacks in MANET and compared various techniques to overcome the attacks[1]. Tushar Sharma et al discussed various techniques but focused on improving the limitations of watch dog, one of the popular technique in IDS[3]. An Intelligent Intrusion Detection and Prevention system for MANET was discussed by Opinder singh et al[5][17][18]. Various attacks and challenges in MANET was discussed[2][19]. The proposed technique dealt with black hole, flooding and selective packet drop attacks in MANET[5]. Vijayarani and Maria Sylviaa discussed various attacks that prevailed in MANET and techniques to overcome those attacks in their study. Nakeeran et al proposed and discussed an agent based intrusion detection system generally for ad hoc networks[6][15][16].

SECURITY ATTRIBUTES AND ATTACKS IN MANET

Security is considered to be an important service of MANET. But ensuring security is really a challenging task in MANET because of its mobility.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 3, 2021, Pages. 2444 - 2452
Received 16 February 2021; Accepted 08 March 2021.

Few attributes which contribute to the security are availability, authenticity, reliability, confidentiality, scalability and integrity.[2] Availability indicates the usage of resources in an efficient way. Authenticity provides authentication for the user or a node. Scalability ensures the network without damage when new node is added to the network. Confidentiality protects the data from unauthorized users. Integrity ensures the trust that original message is received at the other end without corruption. It is important that any of the technique that is used for ensuring he security in a network should not compromise the above listed security attributes.

The following are the common attacks in MANET. The attacks are grouped based on techniques and consequences.

Black hole: Packet is dropped in between during the communication. The place it dropped is not known and hence black hole.

DoS attack: SYN attack, Ping of death, Eavesdropping Attacks, Spoofing attacks, Application level attacks are some attacks that comes under DoS attacks.

Flooding attack: malicious nodes transmit packets continuously to create unnecessary traffic in the network which degrades the performance of the network.

Selective dropping: dropping packets from source to destination. This is an attack which drops few among the bundle of packets during transmission. This is difficult to detect because only selective packets are dropped and remaining packets are untouched and deliver correctly.

Routing loop attack: this attack creates a loop among the routers where the packets revolve round into a single path.

Collaborative attack: two or more nodes act simultaneously to induce an attack is called collaborative attack.

INTRUSION DETECTION SYSTEM TECHNIQUES

WATCH DOG

Watch dog is a method that identifies and detects the misbehaving node. The name watch dog indicates the behaviour of the IDS method. As the name suggest, watch dog watches the packets during transmission. When the source node starts its transmission, the watch dog starts monitoring the packet. The next node within the range and does not forward the same packet then the node is tagged as miscellaneous. The failure tally is increased. If the tally reaches a threshold, then the node is detected as malicious node.

TWO ACK

When there is a communication happening between two nodes and during packet transmission, the destination node of next hop sends back two hop acknowledgement to indicate successful transmission. This is called Two ACK where ACK stands for acknowledgement.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 3, 2021, Pages. 2444 - 2452
Received 16 February 2021; Accepted 08 March 2021.

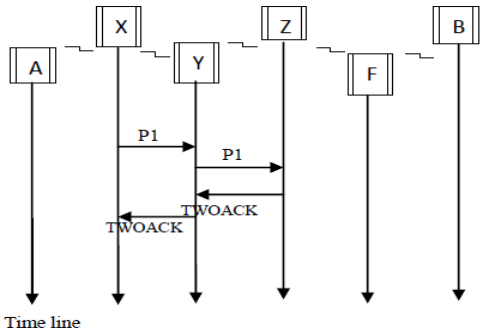

Fig: Two ACK IDS

In the above diagram, when node X transmits the packet to node Y and then to node z. Since node Z is in two hops, it sends two acknowledgements to Y and to X. If there is no acknowledgement, X waits for a time. If the waiting time exceeds the threshold, both the nodes Y and Z are reported malicious.

End to End ACK

It is purely acknowledgement based. The source node once after transmitting packet, expects for acknowledgement from the destination node which is similar to packet transmission hop by hop in the same path through which the packet has been transmitted. In successful reception of the acknowledgement from the destination, the source node transmits the remaining packets.

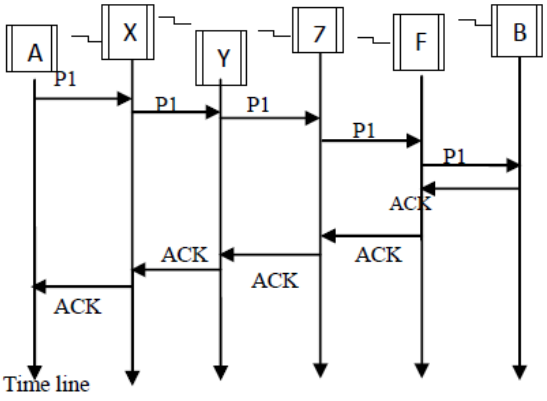

Fig: End to End ACK

AACK

AACK stands for Adaptive Acknowledgement scheme. AACK is a hybrid combination which combines the Two ACK and End to End ACK schemes. Initially when the communication begins between the nodes, the scheme followed will be End to End ACK. In unsuccessful transmission where the acknowledgement packet is not received by the source, the transmission is switched to Two ACK technique.

ZONE BASED INTRUSION DETECTION SYSTEM

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 3, 2021, Pages. 2444 - 2452
Received 16 February 2021; Accepted 08 March 2021.

It falls under anomaly based detection and follows Markov chain model construction. Extracting features, pre processing data, engine construction and tuning the parameters are included. In zone based IDS, the nodes are divided into two zones. The node which connects to other zone physically is called gateway node and all other nodes are called intra zone nodes. There may be more than one gateway node which continuously checks the network for any false packets or acknowledgements. This is to avoid single point failures. Only gateway nodes can alarm the network.

EAACK

The Enhanced Adapted ACKnowledgment is an advanced version of AACK which avoids receiver collision, transmission power reduction and over hearing identification. This three factors form the major drawbacks which declines the performance of the network and security.

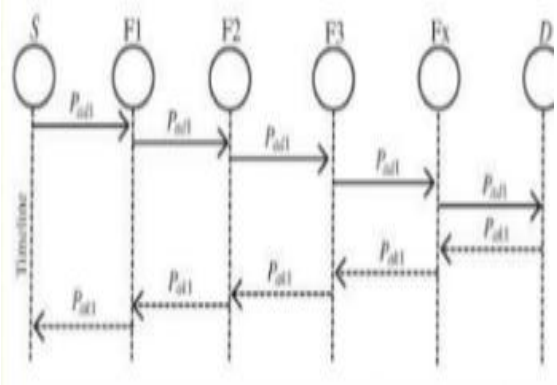

Fig: Enhanced Adaptive Acknowledgement

The EAACK has three major parts. They are ACK, SACK (Secure ACK), MRA (Misbehaviour Report Authentication). The link between two nodes involved in communication is bidirectional. ACK Acknowledgement is end to end. Before transmitting the packets, the source node is expected to send an acknowledgement signal to the destination. If the packet passes through all intermediate nodes and successfully reach the destination, the acknowledgement for the packet sent by the source will be transmitted by the destination node. The acknowledgement from the destination node travels through the same route the first packet came, to the source node. If the packet from destination reaches within a time, then the source starts transmission assuming no malicious nodes in between. If the time exceeds the threshold, then the scheme switches to SACK.

SACK, similar to ACK uses three consecutive nodes for detecting unauthorised users. The third node should send the acknowledgement packets.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 3, 2021, Pages. 2444 - 2452
Received 16 February 2021; Accepted 08 March 2021.

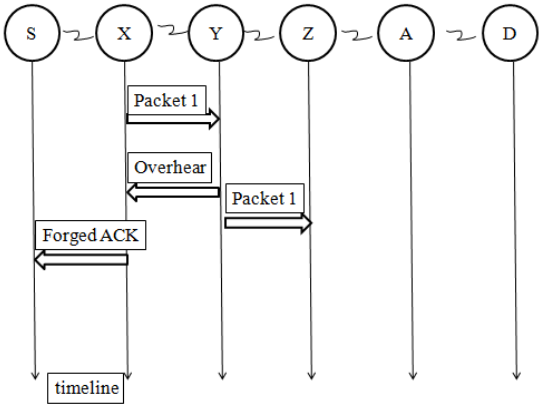

Fig: False misbehaviour report

MRA is the important step in identifying malicious node. If a node is suspected to be malicious, MRA field gets activated. To initiate MRA field, the source first gets the routes to the destination. If the packet is received correctly, then the MRA generated is false. If not there is a malicious node on the route in which the packet is travelled. In addition to the three fields of EAACK, Digital signature is also used for enhancing security using EAACK. An algorithm like RSA can be used. Before transmitting the packets, the ACK packets should be signed digitally and are verified and accepted. Comparing RSA, DSA suits well for digital signature schemes in MANET. The computational power is high comparing RSA but when considering performance and battery power still DSA is preferable.

COMPARISON OF VARIOUS INTRUSION DETECTION SYSTEMS

SCHEME	ADVANTAGES	DISADVANTAGES
Watch dog	Detect misbehaviour node at forwarding stage	Collisions, false MRA, dropping of packets, reduced transmission power
Two ACK	Avoids receiver collision, limited transmission power	Acknowledgement packets reduce the performance by creating unwanted traffic.
End to end ACK	Reduces the overhead caused by the ack packets.	No guarantee for valid acknowledgement packets.
AACK	Avoids receiver collision, less acknowledgement overhead.	If false MRA, then switches to Two ACK causing overhead
Zone based	All nodes simply transmit the packets. Only gateway nodes bother about malicious nodes. No centre point failure.	Only gateway nodes detect the malicious nodes. If attacked in intermediate nodes, it would be difficult to find.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 3, 2021, Pages. 2444 - 2452
Received 16 February 2021; Accepted 08 March 2021.

EAACK	Avoids receiver collision, transmission power reduction, and false misbehaviour identification.	False MRA identification is difficult. Using digital signature also overcomes the drawback.

Table: Comparison of different IDS methods

CONCLUSION

It is clear that only detection mechanisms in MANET do not helps for a successful network with high security. Prevention measures are also needed. We studied various schemes under Intrusion Detection System out of which EAACK was found suitable for many applications in MANET. This paper studied various schemes of intrusion detection system. Though prevention is required than detecting, the detecting should be analysed from the other side before an attacker could attack and damage the system. Concluding this paper, Hybrid architecture can tackle the situation in a better way.

REFERENCES

[1]Ankita sharma, darshanaa birkad et al, implementation of policy enforcement technique for intrusion detection system using manet's,International Journal of Advanced Computational Engineering and Networking, Volume-3, Issue-5, May-2015.

[2] Rajeshkumar, valluvan, A Comparative Study of Secure Intrusion-Detection Systems for Discovering Malicious Nodes on MANETs, International Journal of Computer Applications, Volume 67– No.18, April 2013.

[3]Tushar Sharma et al, An Improved Watchdog Intrusion Detection Systems In Manet,International Journal of Engineering Research & Technology,Vol. 2 Issue 3, March – 2013.

[4]Opinder singh et al, An Intelligent Intrusion Detection and Prevention system for MANET ,Indian Journal of Science and Technology, Vol 10(14),April 2017.

[5]Binod Kumar Pattanayak, Mamata Rath A Mobile Agent Based Intrusion Detection System Architecture For Mobile Ad Hoc Networks, Journal of Computer Science, 2014.

[6] R. Nakkeeran, T. Aruldoss Albert and R.Ezumalai, Agent Based Efficient Anomaly Intrusion Detection System in Adhoc networks, International Journal of Engineering and Technology Vol. 2, No.1, February, 2010.

[7] J.Visumathi, K.L.Shanmughanathan, An effective IDS for MANET using forward feature selection and classification algorithms, International conference on modeling optimization and computing, Procedia Engineering 38, 2012 .

[8] Insha Majeed, Sakshi Arora, An Intrusion Detection System for MANETS, International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 2017.

[9] G.L.Anand Babu, G.Sekhar Reddy, Swathi Agarwal, Intrusion Detection Techniques in Mobile Ad hocNetworks,International Journal of Computer Science and Information Technologies, 2012.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 3, 2021, Pages. 2444 - 2452
Received 16 February 2021; Accepted 08 March 2021.

[10]Shweta Jadye, Survey of MANET Attacks, Security Concerns andMeasures, International Journal of Computer Science and Information Technologies, 2016.

[11]Abdulsalam Basabaa, Tarek Sheltamia and Elhadi Shakshuki, Implementation of A3ACKs intrusion detection system undervarious mobility speeds, Procedia Computer Science, 2014.

[12] Shengyi Pan,Thomas MorrisUttam Adhikari, Developing a Hybrid Intrusion Detection SystemUsing Data Mining for Power Systems, IEEE TRANSACTIONS ON SMART GRID, 2015.

[13]Ehsan Amiri, Hassan Keshavarz, Hossein Heidari, Esmaeil Mohamadi, IntrusionDetection Systems in MANET: A Review, Procedia - Social and Behavioral Sciences, 2013.

[14]Shona D, Dr. M. Senthil Kumar Survey on Intrusion Detection Techniques in MANETs,International Journal of Advance Research inComputer Science and Management Studies, 2015.

[15]Ponmagal, R.S., Karthick, S., Dhiyanesh, B. et al. Optimized virtual network function provisioning technique for mobile edge cloud computing. J Ambient Intell Human Comput (2020).

[16]Ramamoorthy, S., Ravikumar, G., Saravana Balaji, B. et al. MCAMO: multi constraint aware multi-objective resource scheduling optimization technique for cloud infrastructure services. J Ambient Intell Human Comput (2020).

[17]Basha, A.J., Balaji, B.S., Poornima, S. et al. Support vector machine and simple recurrent network based automatic sleep stage classification of fuzzy kernel. J Ambient Intell Human Comput (2020)

[18]Balaji, B.S., Balakrishnan, S., Venkatachalam, K. et al. Automated query classification-based web service similarity technique using machine learning. J Ambient Intell Human Comput (2020)

[19]Viji, C., Rajkumar, N., Suganthi, S.T. et al. An improved approach for automatic spine canal segmentation using probabilistic boosting tree (PBT) with fuzzy support vector machine. J Ambient Intell Human Comput (2020).