ISSN: 2321-7782 (Online)
Volume 3, Issue 10, October 2015
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

A Survey on Intrusion Detection Techniques in MANETs

Shona D[1]
Research Scholar
Research and Development Center
Bharathiar University, Coimbatore, India

Dr. M. Senthil Kumar[2]
Assistant Professor and Head,
S.S. Govt Arts College,
Tiruttani, India

Abstract: In a multi-path wireless network like ad hoc network, co-operation is considered as a significant entity for reliable data dissemination. Since, MANET is highly vulnerable to attack than its wired counterparts. Further, attacks with malicious intent greatly intensify and exploits the vulnerabilities of the network which in turn cripples the performance of MANET. The techniques used possess a low capability of classifying attacks based on the degree of impacts produced by them towards the resilience of the network. For this reason, a need for innovating a set of comprehensive mechanism to prevent the possible attacks of MANET in a flexible way as analogous to the "detect and response" scheme like intrusion detection. This paper aims to explore and classify the current techniques of Intrusion Detection System on various network layer attacks that directly affect the performance of the network by reducing the packet delivery rate, throughput of the network.

Keywords: MANET, Intrusion Detection (IDS), Trust, Attack.

I. INTRODUCTION

Fixed backbone wireless model comprises of a large number of mobile nodes and relatively fewer but more powerful, fixed nodes. The communication between a fixed and a mobile node is through the wireless medium. Nevertheless, this requires a fixed permanent infrastructure.

On the other hand, a Mobile Ad hoc NETwork (MANET) [5,2] is a wireless network consisting of mobile nodes communicating with each other in a multi-hop fashion without the support of any underlying infrastructure such as Base Stations (BSs), wireless Gateways or Access Points (APs) [5,25]

It does not have any centralized administration or fixed network infrastructure. As the transmission range of each low-power node is limited to each other's proximity, the communication to out-of-range nodes are routed through intermediate nodes.

The nodes move freely and communicate over bandwidth-constrained wireless links. Due to self-organization and limited availability of resources, they are subjected to security and selfishness issues.

It is a cost effective solution for communication in disaster recovery activities, military fields or some crisis management services. MANETs support dynamic topologies but have energy and bandwidth constraints, and limited physical security.

Security in Manets

MANETs are highly prone to physical security threats than wireless networks because of its distributed nature. There is an increased possibility of eavesdropping, spoofing, masquerading and Denial-of-Service (DoS) attacks.

MANETs rely on individual security solutions in each mobile node and hence centralized security control is hard to implement. Ensuring security in a MANET is an uphill task due to several factors like vulnerabilities, lack of a priori trust and infrastructure and necessity for cooperation.

Section 2 deals with the attacks in each layer. Section 3 discusses about various intrusion detection techniques and Section 4 gives the conclusion.

II. Attacks in Each Layer

The attacks in MANETs are classified into two mainly two categories namely, passive and active attacks.

- Passive attacks are launched by the adversaries solely to snoop the data exchanged in the network, but never disturb the operation of the network. It is difficult to trace out such attacks as the network is not affected.
- Active attacks try to alter or destroy the information that is being exchanged, thereby disturbing the normal functionality of the network.

MAC LAYER

1. Jamming: Jamming is the main attack in the MAC layer. The attacker keeps monitoring the wireless medium to comprehend the frequency at which the destination node is receiving signals from the sender. It then transmits signals on the same frequency, thus hindering error-free reception at the receiver.

NETWORK LAYER

There are a number of Network layer attacks. The key attacks are discussed below.

1. Wormhole Attack: In wormhole attack, the attacker tunnels the packets from one end to another, and then replays them into the network from that point. Routing is disrupted when control messages are tunneled. The tunnel between two colluding attacks is known as a wormhole.

2. Blackhole Attack: In Blackhole attack, the attacker uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. It listens to the route requests in a flooding based protocol and creates a reply consisting of an extremely short route. If the reply reaches the instigating node before the reply from the actual one, a fake route gets created. Once the malicious node becomes a part of communication, it can intercept packets transferred between authorized nodes.

3. Sinkhole Attack: In case of Sinkhole attacks, the compromised nodes attract data to themselves from all neighboring nodes. By impersonating its neighbors, the adversary gains access to the data flowing through the network. Sinkhole attack is the basis of other attacks like eavesdropping or data alteration. They make use of the loopholes in routing and present themselves as the most attractive partner in a multihop route. Multipath routing aids in overcoming sinkhole attacks. Probabilistic protocols consider the probabilities of packets arriving from a particular source to compute trustworthiness.

4. Flooding Attack: Flooding attack exhausts the network resources such as bandwidth, consumes node's resources such as computational and battery power, disrupts the routing operation and causes severe degradation of network performance. A malicious node sends large number of Route REQuests (RREQs) in a short period to a non-existent destination. As a result, the battery power as well as network bandwidth is consumed leading to DoS attacks.

5. Selfish Node Attack: In Selfish node attack, the nodes in the network do not forward packets to their neighbors so as to conserve their own energy, but attempt to send the packets of their own. It expects service from other nodes but does not destroy or harm the network. There are three types of selfish node attacks. In the first type, the selfish node actively participates in route establishment and denies to forward data packets. In the second type, the selfish node neither participates in route establishment nor forwards data packets. Whereas in the third type, the selfish node participates in routing but drops data packets due to limited availability of energy.

TRANSPORT LAYER

There are only a few Transport layer attacks as discussed below.

1. Session Hijacking Attack: Session hijacking gives an opportunity to the malicious node to behave as a legitimate system. As the communications are authenticated at the beginning of session setup, the attacker hijacks sessions. Initially, he spoofs the IP address of the target machine and finds the correct sequence number followed by a Dos attack. As the target system becomes unavailable, the attacker continues the session with another system as a legitimate one.

2. SYN Flooding Attack: The SYN flooding attack is a DoS attack, wherein the attacker creates a large number of half-opened TCP connections with a victim node, but never completes the handshake to fully open the connection. The malicious node sends a large amount of SYN packets to the victim, spoofing the return addresses of the SYN packets. The victims on the other hand send SYN-ACK once they receive the SYN packets from the attacker and wait for the response of ACK packet. As the ACK packets are not set as responses, the half-opened connections overflow the buffer. The victim is now in a predicament unable to accept any legitimate attempts to open a connection. Normally, time-outs are executed with pending connections and the half-open connections eventually expire. Even though the victim nodes recover, the malicious nodes simply continue sending packets that request new connections faster than the expiration of pending connections.

APPLICATION LAYER

The attacks in the application layer include mobile viruses, worm attacks, and repudiation attacks.

1. Mobile Virus and Worm Attacks: The application layer contains user data, and supports many protocols such as HTTP, SMTP, FTP. Malicious code including viruses and worms is applicable across operating systems and applications. There are a number of techniques by which a worm can discover new machines to exploit. One example is IP address scanning used by Internet worms, wherein probe packets are generated to a vulnerable UDP/TCP port at many different IP addresses. Hosts that are hit by the scan respond receive a copy of the worm and hence get infected. An attacker can produce a worm attack using any loophole of the system of the MANET.

2. Repudiation Attack: In the network layer, firewalls keep packets in or out. In the transport layer, entire connections can be encrypted, end-to-end. But these solutions do not solve the authentication or non-repudiation problems in general. Repudiation refers to a denial of participation in all or part of the communications.

ATTACKS ON MULTIPLE LAYERS

Some security attacks involve more than one layer instead of a particular layer. Such multi-layer attacks include DoS, Man-In-The-Middle and impersonation attacks.

1. Denial of Service (DoS) Attack: Denial of service (DoS) attacks can be launched from more than one layer. An attacker can employ signal jamming at the Physical layer disrupting normal communications. At the MAC layer, malicious nodes can occupy channels preventing other nodes from channel access. At the Network layer, the routing process can be interrupted by routing control packet modification, selective dropping, table overflow or poisoning. At the Transport and Application layers, SYN Flooding, Session Hijacking and malicious programs can cause DoS attacks.

2. Man-In-The-Middle Attacks: An attacker sniffs the information sent between the sender and the receiver. In some cases the attacker may impersonate the sender to communicate with the receiver, or impersonate the receiver to reply to the sender.

III. Intrusion Detection Mechanisms for Mitigating Network Layer Attacks

Many mechanisms are proposed in the literature to mitigate attacks in different layers. This work mainly focuses on the attacks in the Network layer as mentioned in the previous section. The classical intrusion detection mechanisms mainly fall under four categories as listed below.

- Fuzzy based intrusion detection
- .Neural networks based intrusion detection
- Agent based intrusion detection
- Trust based intrusion detection

FUZZY BASED INTRUSION DETECTION

The idea of fuzzy logic, a method to deal with uncertainty and reasoning alike human reasoning was introduced by Dr. Lotfi Zadeh, University of California, Berkeley in the 1960s (Zadeh 1965)[26].

Fuzzy logic, a form of many-valued logic, has truth values of real numbers ranging from '0' to '1'. In case of Boolean logic, the truth values of variables may be either '0' or '1'. The values '0' and '1' are considered as extreme cases of truth and various states of truth are considered to be in-between. To be precise, fuzzy logic handles truth partially, where the truth values may range between 'completely true' and 'completely false' [12].

Since fuzzy logic can deal with uncertainty and complexity derived from human reasoning, it is used in modelling the IDS [15]. IF-Then-Else fuzzy rules identify attacks or intrusions in a network.

The fuzzy behavior of attacks was taken into consideration and the Intrusion Detection System (IDS) was developed based on it.

Stationary Intelligent Fuzzy Agents (SIFA) was proposed by Domian Walkins [24] to detect distributed DoS attacks in MANETs. The dynamic topology of MANETs demands SIFA to reside in each node. Rules are written and an interference engine is used to perform reasoning by processing the database of derived facts.

SIFA demands processing at each node. Fuzzy Based Response Model (FBRM) is proposed to detect internal attacks in MANETs like False Route Request (FRR) that leads to flooding, congestion, DoS attack, exhaustion of bandwidth [19]. To predict the FFR attack, a Fuzzy logic controller is used to monitor various features like route request rate, sequence number, acknowledgement time and load pattern. It includes a log file that contains information about various features of the local node as well as its neighbors. The Level of Hacking (LOH) is computed from the sequence number, Route REQuest (RREQ) rate and acknowledgement time.

The previous works did not address the Black hole attack which is a predominant attack in the network layer. The fuzzy logic based IDS proposed by Kulbhushan & Jagpreet [9] to detect black hole attack on MANETs uses the rules based on Mamdani fuzzy model. It generates the membership function using forward packet ratio and average destination sequence number selected in each time slot. The output of the derived rule is based on the fidelity level of each node ranging from 0 to 10. The threshold value for fidelity is set to 5.5. The nodes with fidelity level of nodes less than or equal to the threshold are prone to be black holes.

To determine the level of maliciousness, some authors designed IDS using fuzzy variables. Intrusion detection features can be represented using fuzzy variables and the network behavior can be analyzed based on the fuzziness that shows the degree of maliciousness of a node [21].

A Fuzzy Interference System (FIS) is designed for detecting the Black hole attack [23]. Selection of appropriate clustering algorithm in IDS using FIS plays a vital role. In this paper, the authors have compared the performance of subtractive and Fuzzy c-mean clustering. They have concluded that subtractive clustering is more efficient than the fuzzy c-means clustering.

Similarly, Sarah and Nirkhi [1] introduced fuzzy logic based intrusion detection scheme to detect the Distributed Denial-of-Service (DDoS) attacks based on Dynamic Source Routing (DSR) protocol. The authors have used forensic analysis to detect intrusions, gather digital evidences from any compromised system, and reconstruct the compromised system to identify the location of the attacker. The log files are captured, analyzed using fuzzy logic and a forensic report is prepared.

NEURAL NETWORKS BASED INTRUSION DETECTION

Chavan et al [14] developed IDS that uses Fuzzy Inference System and Artificial Neural Networks (ANN). The system is trained by creating a signature pattern database using Protocol Analysis and Neuro-fuzzy learning method.

Classification yields better results. Mitrokotsa et al [11]) have proposed an intrusion detection scheme based on Neural Networks and Watermarking techniques. The local IDS agent includes a data collector and intrusion detection engine. The data collector collects local audit data and activity logs, while the intrusion detection engine detects the local anomalies using local audit data. The emergent Self-Organizing Maps (eSOMs) classification algorithm performs local anomaly detection. The labeled audit data is selected and appropriate transformations are performed. The classifier is computed using the training data and the eSOM algorithm. The classifier is applied to test local audit data and classify it as normal or abnormal. Finally, watermarking is done in the local eSOM map so as to ensure that it is not modified and prove the existence of intrusions locally in a node.

AGENT BASED INTRUSION DETECTION

The cluster-based IDS proposed by Kachirski & Guha [7] uses mobile agents to perform monitoring, take decisions or action. Sensors monitor the network and agents take decisions. Packet monitoring is performed in a few nodes thus reducing the IDS-related processing time.

To extend coverage, Albers et al [2] proposed architecture for intrusion detection. It detects intrusions locally using mobile agents. The local intrusion detection agent at each node can be extended to deal globally by cooperating with other local agents. Security data and intrusion alerts are exchanged among local agents.

To reduce the amount of communication in the process of intrusion detection, a two-level non-overlapping Zone-Based Intrusion Detection System (ZBIDS) for anomaly detection was propounded by Sun et al.[20]. Inter-zone nodes collect and aggregate the reports and alerts from intra-zone nodes, while the inter-zone node team up and perform intrusion detection in more than one zone, thus increasing the detection rate and reducing the false positive alarm.

To increase the number of nodes, a scalable dynamic intrusion detection hierarchy using clustering is proposed by Sterne et al. [18]. It resembles the methodology proposed by Kachirski & Guha (2002), but involves more than two levels involving cluster heads and leaves. Each node monitors, prepares logs, analyses, responds to intrusions detection and forwards reports to the cluster heads. The cluster heads are responsible for performing data fusion/integration, data filtering, computations related to intrusion detection and security management.

The challenges and characteristics of pervasive computing devices are discussed by Kannadiga et al [8], Further, Agent-based IDS for pervasive computing environments that consider the scarcity and heterogeneity of computing resources based on static and a mobile agent is designed.

In FORK, proposed by Ramachandran et al [14], many mobile agents are involved. Only the nodes with resources that are capable of performing intrusion detection compete and get the IDS agent tasks. Task allocation is done by auctioning. Whenever a node identifies certain changes in a network, it initiates auction submitting auction requests to the network. The interested nodes respond by forwarding their willingness to the initiating node, which performs a selection based on several metrics including battery power metric. The selected nodes detect intrusions using the Ant Colony Optimization (ACO) algorithm. No information about the security of the mobile agents is given in the mechanism.

TRUST BASED INTRUSION DETECTION

Trust based intrusion detection schemes gain their popularity as the trustworthiness of a node determines the security of a network.

In the reputation based protocol namely CONFIDANT proposed by Buchegger & Boudec [3] for the Dynamic Source Routing (DSR) protocol, two lists are maintained by each node to deal with the selfish nodes. The neighbors are monitored and their selfish behavior is reported. Rational nodes are added to the friends list and the nodes which drop or tamper the packets or tamper are added to the black list. The trust is calculated based on the lists that are exchanged between the neighboring nodes and the packets are not forwarded to a node when its trust falls below a certain threshold. It performs inconsistent evaluation, wherein the evaluation of each node varies, thus considering a node to be selfish when others do not. The former behavior of the nodes is not taken into consideration once misbehavior is predicted.

The Collaborative REputation (CORE) Mechanism proposed by Michiardi & Molva [13] performs combined and distributed local observations to compute the reputation for each node, based on which, the nodes are either allowed to be a part of the network or excluded. The nodes collaborate to obtain the global reputation value by combining the local reputation values and react to negative reputations of nodes. The outcome of a function comprising of the experiences of a node and its neighbors is computed. The rating of a node is changed if the behavior of a node drifts from the outcome.

Some mechanisms are proposed in the literature to give incentives to the unselfish nodes. Secure and Objective Reputation-Based Incentive (SORI) scheme proposed by He et al [6] restrict selfish behavior. This protocol maintains two records namely, the local and the overall evaluation record containing the reputation index given by the neighbor nodes to detect and exclude the selfish nodes.

To ensure privacy among nodes based on trust, a trust relationship based on the node behavior establishes an association between trusting and trusted nodes Schmidt et al [17]. The node whose trustworthiness is to be ensured is called the trusted node and the node that evaluates a node's trustworthiness is the trusting node. The nodes that share their experiences to the entreating nodes are called the recommending nodes.

It is better to define a mechanism that does not use Central authorities to rate the trustworthiness of other nodes. A fuzzy trust recommendation based on collaborative filtering is proposed by Luo et al [10] to stimulate collaboration among nodes, detect untrustworthy nodes and assist decision-making in various protocols. As fuzzy logic deals with uncertainty and inaccurate information, a trust model that combines trust and trust recommendation information based on collaborative filtering is designed.

An energy based trust management scheme that detects selfish nodes using fuzzy logic is proposed by Vijayan et al. [22]. Each node monitors its nearest neighbor for detecting the malicious behavior. The scheme involves a supervisor module that passively listens to the neighbor's communication using Passive Acknowledgement (PACK) mechanism to keep track of the packets that are forwarded. The trust level is calculated based by the Aggregator module based on the number of packets dropped. The percentage of packets dropped is taken as the fuzzy input variable.

IV. Conclusion

This paper has presented the possible categories of intrusion detection systems that are structured to be distributed and co-operative in identification. Moreover, the aim of each intrusion detection system with their significance and application on mobile nodes or intrusions into the networks are portrayed. Besides the impact of each attack, the root cause of attacks and the entity that would be compromised by that attack with their influential degree are also explained. Finally, an extract and future focus on a variety of research directions are enumerated for analysis.

References

1. Ahmed S & S.M. Nirkhi S M, “A Fuzzy approach for forensic analysis of DDoS attack in manet”, International Conference on Computer Science and Information Technology, ISBN: 978-93-82208-70-9, Hyderabad, 10th March 2013.

2. Albers P, Camp O, et al, “Security in Ad Hoc Networks: a General Intrusion Detection Architecture Enhancing Trust Based Approaches”, Proceedings of the 1st International Workshop on Wireless Information Systems (WIS-2002), 1-12.

3. Buchegger S and Boudec J Y L, “Performance analysis of the confidant protocol,” in MobiHoc ’02: Proceedings of the 3rd ACM international symposium on Mobile ad-hoc networking & computing, New York, NY, USA: ACM, 2002, pp. 226–236.

4. Charles E. Perkins, editor. Ad Hoc Networking. Boston: Addison-Wesley, 2001

5. Corson. S and Macker. J, “Mobile Ad Hoc Networking (MANET): Routing protocol performance issues and evaluation considerations”, Jan. 1999, IETF RFC 2501.

6. He Q, Wu D, Khosla P , SORI, “ A secure and objective reputation- based incentive scheme for adhoc networks”, In Proceedings of IEEE WCNC2004, March 2004.

7. Kachirski O, and Guha R, “Intrusion Detection Using Mobile agents in wireless Ad hoc Networks”, In Proc. of the IEEE workshop on Knowledge Media Networking, July 2002, Kyoto Japan, pp.153-158.

8. Kannadiga P, Zulkernine M and Ahamed S, “Towards an Intrusion Detection System for Pervasive Computing Environments”, In Proc. of the International Conference on Information Technology (ITCC’05), Las Vegas, Nevada, April 2005, pp. 277-282.

9. Kulbhushan and Jagpreet Singh, “Fuzzy logic based intrusion detection system against black hole attack AODV in manet”, IJCA Special issue on “Network Security and Cryptography” Vol. NSC(No. 2),2011, pp. 28-35.

10. Luo J, Liu X, Zhang Y, Ye,D, & Xu, Z, “Fuzzy trust recommendation based on collaborative filtering for mobile ad-hoc networks”. IN LCN, October 2008, pp. 305-311

11. Mitrokotsa A., Komninos N and Douligeris C, “Intrusion detection with neural networks and watermarking techniques for MANET” In Pervasive Services, IEEE International Conference July 2007, (pp. 118-127).

12. Novak V, Perfilieva I and Mockor J, “Mathematical principles of fuzzy logic Dodrecht: Kluwer Academic. ISBN 0-7923-8595-0.

13. Pietro Michiardi and RefikMolva, “Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad-hoc networks,” in Proceedings of the IFIP TC6/TC11 Sixth Joint Working Conference on Communications and Multimedia Security. Deventer, The Netherlands, The Netherlands: Kluwer, B.V., 2002, pp. 107–121.

14. Ramachandran C, Misra S and Obaidat M S, “FORK: A novel two-pronged strategy for an agent-based intrusion detection scheme in ad-hoc networks”, Computer communications, 2008, 31(16), 3855-3869.

15. Shanmugam, B and Idris N B, “Anomaly Intrusion Detection based on Fuzzy Logic and Data Mining”, In Proceedings of the Postgraduate Annual Research Seminar, Malaysia 2006.

16. Sampada Chavan**,** Khusbu Shah, Neha Dave, Sanghamitra Mukherjee, Ajith Abraham, Sugata Sanyal, “Adaptive Neuro-Fuzzy Intrusion Detection Systems”, IEEE International Conference on Information Technology: Coding andComputing,2004 (ITCC ’04), Proceedings of ITCC 2004, Vol. 1, April, 2004, Las Vegas, Nevada, pp. 70-74.

17. Schmidt S, Steele S, Dillon T S , and E. Chang, “Building a fuzzy trust network in unsupervised multi-agent environments,” in OTM Workshops, 2005, pp. 816–825.

18. Sterne D, Balasubramanyam P and et al. “A General Cooperative Intrusion Detection Architecture for MANETs” Proceedings of the 3rd IEEE International Workshop on Information Assurance (IWIA'05), 2005, 57-70.

19. Sujatha S, Vivekanandan P, Kannan A, “Fuzzy logic controller based intrusion handling system for mobile adhoc networks”, Asian Journal of Information Technology, 2008, pp.175-182.

20. Sun B, Wu K, and Pooch U W , “Alert Aggregation in Mobile Ad Hoc Networks”, Proceedings of the 2003 ACM Workshop on Wireless Security (WiSe'03) in conjunction with the 9th Annual International Conference on Mobile Computing and Networking (MobiCom'03), 69-78.

21. Verma A, Anil K R , and Om Prakash Jain. "Fuzzy Logic Based Revised Defect Rating for Software Lifecycle Performance Prediction Using GMR.", Bharati Vidyapeeth’s Institute of Computer Applications and Management, 2009.

22. Vijayan R, Mareeswari V and Ramakrishna K, “Energy based trust solution for detecting selfish nodes in manet using fuzzy logic”, International Journal of research and reviews in computer science ,Volume: 2(No. 3), June 2011,pp. 647-652.

23. Vydeki D and Bhuvaneswaran R S “Effect of clustering in designing a fuzzy based hybrid intrusion detection system for mobile ad hoc networks”, Journal of Computer Science, Vol. 9(No. 4),2013, pp. 521-525.

24. Watkins, Damian. "Tactical manet attack detection based on fuzzy sets using agent communication.”In 24th Army Science Conference, Orlando, FL, 2005.

25. Yu, F. R., “Cognitive Radio Mobile Ad Hoc Networks”. New York, NY, USA: Springer-Verlag, 2011.

26. Zadeh L A "Fuzzy sets". Information and Control 8 (3) ,1965, 338–353. doi:10.1016/s0019-9958(65)90241-x.

AUTHOR(S) PROFILE

Shona D, is a research scholar at Bharathiar University. She received her M.Phil degree in Computer Science from Bharathiar University, MCA degree from Bharathiar University. Her area of specialization is security in MANET.

Dr M.Senthil Kumar, received his Doctorate in Computer Science from Anna University. He is now Head and Professor of Computer Science Department, SS Govt Arts College, He has done his PhD to ensure the Quality of Service while routing through MANET. He has published many papers regarding in his broad field research. His area of specialization includes Networking, Cloud Computing, and Software Engineering.