ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 1, Issue 7, September 2012

A Survey on Enhanced Intrusion Detection System in Mobile Ad hoc Network

Shankar Sharan Tripathi, Sonu Agrawal

Abstract— **In the last few years, we have seen the fast development of wireless communication technologies and a mobile ad hoc network play a major role for wireless communication. A MANET is a self-determining collection of mobile nodes that communicate over comparatively bandwidth constrained wireless mediums. Since the nodes are mobile, the network topology may change rapidly and impulsively over time. Many critical applications are using the mobile ad hoc network; therefore, security issue has become one of the major concerns in MANETs. Due to some unique features and characteristics of MANETs, prevention methods alone are not sufficient to make them secure; therefore, detection should be added as another defense before an attacker can break the system. Intrusion detection is an important technology in business sector as well as an active area of research. It is an important tool for information security. An Intrusion Detection System is used to supervise networks for attacks or intrusions and report these intrusions to the administrator in order to take direct action. In this paper we have surveyed different types of intrusion detection techniques in MANETs and analyzed their effectiveness.**

Keywords — Mobile Ad Hoc Network (MANET), Intrusion Detection System (IDS), Security, Intrusion Detection (ID).

I. INTRODUCTION

A mobile ad-hoc network (MANET) is a self-configuring infrastructure less network of mobile devices connected by wireless links. In A Mobile ad hoc network, different wireless mobile devices are working as a mobile node that build virtual network without any centralized administrative for wireless communication. Each device in a MANET is free to move separately in any direction, and will therefore change its links to other devices regularly. Each must forward traffic unrelated to its own use, and therefore be a router [15]. MANETs are highly vulnerable to attacks than wired networks due to the open medium. Security in an infrastructure-less and ad hoc network is a great challenged. At the same time the resources restraints (limited power, limited communication range, processing capabilities, and limited memory) of the mobile devices in the MANETs leads tradeoff between security requirements and resources utilization [8]. Providing security in MANETs is a prime concern due to the need of providing protected communication between mobile nodes in unfriendly environment. Mobile Ad hoc network maximize the total network throughput by using all available nodes for routing and forwarding. Hence, a node can misbehave and fail to establish route or route the data due to its malicious activity to decrease the performance of ad hoc network.

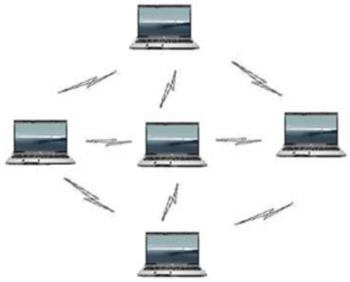

Figure 1: Wireless Network Architecture.

A. *Applications of Ad hoc Networks:*

A MANET is suitable for a wide range of applications. An application of Ad hoc network include [7, 9]:

1) *Sensor Networks:* A Wireless Sensor Network (WSN) consists of spatially distributed self-governing sensors to monitor physical or environmental conditions. A wireless sensor network (WSN) has important applications such as remote environmental monitoring and target tracking. This has been enabled by the availability, particularly in recent years, of sensors that are smaller, cheaper, and intelligent. These sensors are equipped with wireless interfaces with which they can communicate with one another to form a network [10].

2) *Military Tactical operations:* A MANET could be deployed quickly for military communications in the battlefield. Geographical location is one of the important factors of any military operation which makes the current geographical positioning systems; MANET help to create the virtual network which is helpful for military tactical operations.

3) *Emergency Services:* As the internet importance increasing rapidly, A MANET could be easily deploy where the network connectivity has lost due to natural disaster.

B. *Characteristics of Ad hoc Networks:*

Mobile Ad hoc networks are inherently different from well known wired networks. The characteristics of ad hoc networks are as follows [2]:

1) *Dynamic changing network topology:* The nodes in MANETs are free to move at any direction at any time. So the networks topology of the MANETs changes rapidly and randomly at any time.

Manuscript received Sep 15, 2012.

Shankar Sharan Tripathi, *ME Scholar, Deptt. Of Computer Science & Engineering, Shri Shankaracharya College of Engineering & Technology Bhilai, India, +91-8103898111.*

Sonu Agrawal, *Deptt. Of Computer Science & Engineering, Shri Shankaracharya College of Engineering & Technology, Bhilai, India, +91-9926848558.*

2) *Bandwidth constraints:* Wireless links have significantly lower bandwidth than well known wired networks.

3) *Energy constraints:* MANETs also have nodes whose energy storage is very limited. Often, they are battery equipped, with very limited to no recharging or replacement possibility.

4) *Limited security:* MANETs are much more vulnerable to attacks due to their open medium, lack of centralized monitoring, cooperative algorithm and dynamically changing topology.

5) *Node cooperation*: MANETs support cooperative algorithms. In MANETs every node is responsible for routing and forwarding the information to maximize the total network throughput.

6) *Malicious or selfish Behavior*: A node in MANET might act as malicious to disrupt the network by dropping or corrupting the data packets. A node in MANET might be selfish and not willing to spend its battery for the other nodes.

C. Security requirements in MANET:

The security services of ad hoc networks are not altogether different than those of other network communication paradigms. The goal is to protect the information and the resources from attacks and misbehavior. A secure protocol for ad hoc network must satisfy the following requirements [1, 3].

1) *Availability:* ensures that the desired network services are available whenever they are expected, in spite of attacks. Systems that ensure availability seek to combat denial of service and energy starvation attacks that we will present later.

2) *Confidentiality:* is a core security primitive for ad hoc networks which guarantee that information is not accessed by unauthorized persons. It ensures that a given message cannot be understood by anyone else than its (their) desired recipient(s). One of the popular techniques used for ensuring confidentiality is data encryption [1].

3) *Authenticity:* ensures communication from one node to another is genuine. It ensures that a malicious node cannot masquerade as a trusted network node.

4) *Integrity:* denotes the authenticity of data sent from one node to another. That is, it ensures that a message sent from node A to node B was not modified by a malicious node, C, during transmission. If a robust confidentiality mechanism is employed, ensuring data integrity may be as simple as adding one-way hashes to encrypted messages [1].

5) *Non-repudiation:* ensures that the origin of the message is legitimate, that is when one node receives a false message from another, non-repudiation allows the former to accuse the later of sending the false message and enables all other nodes to know about it. One of the most popular techniques used for ensuring non-repudiation is Digital Signatures, which function as unique identifier for each user, much like written signature [1].

Various intrusion detection Systems are developed for detecting the malicious nodes in the wired networks. Due to the mobility of nodes, the intrusion detection techniques of wired network can not be used for MANETs.

Intrusion detection is an important part of computer security. It provides an additional layer of defense against computer, which is used after physical, authentication and access control [6]. An intrusion detection system gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organization) and misuse An Intrusion detection uses vulnerability assessment (sometimes referred to as scanning), which is a technology developed to assess the security of a computer system or network.

Intrusion detection functions include:

- Monitoring and analyzing both user and system activities.
- Analysis of abnormal activity patterns.
- Analyzing system configurations and vulnerabilities.
- Ability to recognize patterns typical of attacks.
- Assessing system and file integrity.
- Tracking user policy violations.

The intrusion detection System monitors the activities of the system, analyze the activities to determine that any of the activity is violating the security rules. Once An IDS determines that an unusual activity or an activity that is known to be an attack occurs, it then generates an alarm to alert the security administrator. In addition, IDS can also initiate a proper response to the malicious activity [14].

Intrusion detection can be classified based on audit data as either host-based or network-based. A network-based IDS captures and analyzes packets from network traffic while a host-based IDS uses operating system or application logs in its analysis. Based on detection techniques, IDS can also be classified into three categories as follows [2].

6) *Anomaly detection systems:* The normal profiles (or normal behaviors) of users are kept in the system. The system compares the captured data with these profiles, and then treats any activity that deviates from the baseline as a possible intrusion by informing system administrators or initializing a proper response.

7) *Misuse or signature detection systems*: The system keeps patterns (or signatures) of known attacks and uses them to compare with the captured data. Any matched pattern is treated as an intrusion. Like a virus detection system, it cannot detect new kinds of attacks [4].

8) *Specification-based detection:* The system defines a set of constraints that describe the correct operation of a program

or protocol. Then, it monitors the execution of the program with respect to the defined constraints.

II. EVOLUTION

Intrusion detection in MANET is one of the most important research areas. In 1984 Fred Cohen noted that it is impossible to detect an intrusion in every case and that the resources needed to detect intrusions grows with the amount of usage.

In 1987 the dinning proposed a model of a real-time intrusion-detection expert system that can able to detect break-ins, penetrations, and other forms of computer abuse. The model is based on the assumption that security violations can be detected by monitoring a system's audit records for unusual patterns of system usage. The model includes profiles for representing the activities of subjects with respect to objects in terms of metrics and statistical models, and rules for acquiring knowledge about this behavior from review records and for detecting anomalous behavior [5].

In 2000, the S. Marti,T.J. Giuli, K. Lai and M. Proposed the "watchdog and Pathrater" scheme that is used to detect & mitigate the effect of nodes that do not forward packets. Watchdog determines misbehavior by replication packets to be forwarded into a buffer and monitoring the behavior of the adjacent node to these packets. Watchdog promiscuously snoops to decide if the adjacent node forwards the packets without modifications or not. If the packets that are snoop match with the observing node's buffer, then they are discarded; whereas packets that stay in the buffer beyond a timeout period without any successful match are flagged as having been dropped or modified. The node responsible for forwarding the packet is then noted as being suspicious. If the number of violations becomes greater than a certain predetermined threshold, the violating node is marked as being malicious. [11].

In 2001 Knowledge-based intrusion detection systems was proposed by H.–Y. Chang, S.F. Wu and Y.F. Jou, which accumulate knowledge about attacks, examine traffic and try to identify patterns indicating that a suspicious activity is occurring. This approach can be applied against known attack patterns only and the utilized knowledge base needs to be updated frequently [12].

In 2002, the Farooq Anjum and Dhanant Subhadrabandhu and Saswati Sarkar propossed a "signature based intrusion detection technique ",in which they assume that they knows the signature of the attack and all the system execute the IDS such nodes are said to constitute the intrusion detection subsystem. [4].

In 2003, O. Kachirski and R. Guha proposed a sensor based approach to detect intrusion. In which multiple sensors are deployed and audit data is collected from all the sensors these data is merged to detect the intrusion [16].

In 2003, Bo Sun,Kui Wu and Udo W. Pooch introduce a geographic zone based intrusion detection frameworks that uses a location aware zone gateways node to collect and aggregate the alerts from intra-zone nodes. Gateway node in neighboring zone cans then further collaborate to perform the intrusion detection in the wide area and to attempt to reduce the false positive alarm [13].

In 2004, D. Sterne, et al. Present a cooperative intrusion detection architecture that facilitates accurate detection of MANET-specific and conventional attacks. The architecture is organized as a dynamic hierarchy in which detection data is acquired at the leaves and is incrementally aggregated, reduced, and analyzed as it flows upward toward the root. The nodes at the top are responsible for security management functions [17].

In 2005, Ioanna Stamouli propossed RIDAN architecture which uses timed finite state machine to formally define attack against the AODV routing process. It uses a knowledge based methodology to detect the intrusion. RIDAN operates locally in every participating node and observe the network traffic. This model can able to detect resource consumption attack, Sequence number attack and dropping routing packet attack [18].

In 2006 Yu Liu, Cristina Comaniciu and Hong Man proposed a Bayesian Game Approach for Intrusion Detection in Wireless Ad Hoc Networks. In this paper, they propose a game theoretic framework to analyze the interactions between pairs of attacking/defending nodes using a Bayesian formulation. They studied the achievable Nash equilibrium for the attacker/defender game in both static and dynamic scenarios [6].

In 2006 A. Karygiannis, E. Antonakakis, and A. Apostolopoulos Proposed a method to detect the critical node for MANET. Critical node is a node whose failure or malicious behavior disconnects or significantly degrades the performance of the network. After identification of critical node, these nodes are continuously monitored. To detect the critical node they used a vertex cut and edge cut approach [19].

In 2006 Xia Wang proposed end to end Wormhole detection method in wireless ah hoc networks. They used AODV protocol. In the route discovery process the sender sets the Destination-only flag such that only the destination can able to respond to the ROUTE REQUEST packet. Once the ROUTE REQUEST packet reaches to the destination, it responds by sending a ROUTE REPLY with its current position. The sender retrieves the receiver's position from the ROUTE REPLY packet and estimates the lower bound of hops between the sender and the receiver. If the received route is shorter than the estimated shortest path, the corresponding route will be discarded. Otherwise, the sender will select the shortest path corresponding to the estimation. After the detection of wormhole by sender, it temporarily enables the path with wormhole and sends the TRACE packet to the receiver through this path. This TRACE packet is forwarded by each intermediate node through the route with wormhole [20].

In 2007, R.Ranjana and M. Rajaram Proposed a model which does not perform any change in underlying protocol and used additional security component to detect fabrication attack, resource consumption attack and packet dropping attack[21].

In 2008 Ningrinla marching and Raja Datta proposed "collaborative technique for Intrusion detection in MANET". In this, they proposed two intrusion detection techniques for mobile ad-hoc networks, which use collaborative efforts of nodes in a neighborhood to detect a malicious node in that neighborhood. The first technique is designed for detection of malicious nodes in a neighborhood of nodes in which each pair of nodes in the neighborhood are within radio range of each other. Such a neighborhood of nodes is known as a clique. The second technique is designed for detection of malicious nodes in a neighborhood of nodes, in which each pair of nodes may not be in radio range of each other but where there is a node among them which has all the other nodes in its one-hop vicinity[2].

In 2009, Sheenu Sharma and Roopam Gupta propossed a "Simulation study of blackhole attack in the mobile ad hoc networks"In this, they investigated the effects of Blackhole attacks on the network performance. they simulated Blackhole attacks in Qualnet Simulator and measured the packet loss in the network with and without a blackhole. The simulation is done on AODV (Ad hoc On Demand Distance Vector) Routing Protocol. The network performance in the presence of a blackhole is reduced [22].

In 2010, A.Rajaram and Dr. S. Palaniswami developed a "Malicious node detection system for mobile ad hoc networks" which includes trust based security protocol based on a MAC-layer approach which attains confidentiality and authentication of packets in both routing and link layers of MANETs. In the first phase of the protocol, they design a trust based packet forwarding scheme for detecting and isolating the malicious nodes using the routing layer information. It uses trust values to favor packet forwarding by maintaining a trust counter for each node. A node is punished or rewarded by decreasing or increasing the trust counter. If the trust counter value falls below a trust threshold, the corresponding intermediate node is marked as malicious. In the next phase of the protocol, they provide link-layer security using the CBC-X mode of authentication and encryption. By simulation results, we show that the proposed MAC-layer security protocol achieves high packet delivery ratio while attaining low delay, high speed and overhead [23].

In 2011, Md. Safiqul Islam and Syed AshiqurRahman developed "Anomaly Intrusion Detection System in Wireless Sensor Networks: Security Threats and Existing Approaches". in which they mention several attacks on WSN and they primarily focus only on the anomaly based intrusion detection system as well as they discuss about several existing approaches to describe how they have identified security threats and implemented their intrusion detection system [24].

III. Challenges in Intrusion Detection System

Many networks are huge and can even contain a various collection of thousands of devices. Sub-components in a large network may communicate using different technologies and protocols. For future research in this area to propose new technologies for intrusion detection in mobile ad hoc networks and some of these are:

- One challenge for IDS devices deployed over a large network is for IDS components to be able to communicate across sub-networks, sometimes through firewalls and gateways.
- Another challenge in a huge network is for the IDS to be able to successfully examine traffic. Network IDS components are scattered throughout a network, but if not placed tactically, many attacks can altogether bypass Network IDS sensors by traversing alternate paths in a network.
- Many common operating systems are simply not designed to operate securely. Thus, malware often is written to exploit discovered vulnerabilities in popular operating systems. Depending on the nature of the attack, many times if an operating is compromised, it can be difficult for an IDS to recognize that the operating system is no longer legitimate.
- IDS accuracy itself is a critical issue. In MANETs, the IDS monitor the activities and analyze and compare them against the security rules and accordingly generate the alarm. Because of the dynamic nature of network, most IDS suffer from the false positive and false negative alarm.
- Unlike wired network, the mobile ad hoc network does not need any infrastructure so it is very complicated to perform any kind of centralized management and control.
- Large numbers of sensors are deployed to monitor the network activities in coordinated intrusion detection techniques and discover most favorable position of the sensors, which requires tactical processing and collecting data from them consumes a lot of network bandwidth.
- The resource constraint constitutes another challenge to mobile ad hoc network. The wireless channel is bandwidth-constrained and shared among many networking entities. At the same point computational capabilities of mobile devices are also limited and these devices are powered by batteries with its inherent limitation.
- One of the Major challenges with wireless is that the new technology comes with its own set of protocols for communication that break the traditional OSI layer model. IDS must learn new communication patterns. Also, as open as wireless communication is, devices on such networks rely on established trust relationships between identified systems.

IV. CONCLUSION AND FURTHER DEVELOPMENT

Today wireless technologies are commonly used across the globe to support the communication needs of a huge number of end users. The importance of wireless technologies in everyday life has been discussed. In this paper, we have discussed about the ad hoc wireless networks and we have seen that MANETs have several advantages over traditional wireless networks such as self-government of fixed infrastructure, ease of use etc. On the other hand we have seen that MANETs are highly vulnerable to attacks due to their characteristics such as lack of centralized control, dynamic topology, limited resources and open media. These features present new challenges for intrusion detection techniques and as such, achieving security in ad hoc network is more difficult compared to wired networks. We also discuss some challenges and difficulty of intrusion detection in MANET. There is a maximum need of a common basis for all intrusion detection and sustaining activities that can able to adjust dynamic network conditions. These activities include detecting all types of attack on MANET.

REFERENCES

[1] William Stallings.”Cryptography and Network Security principles and practices”. Pearson Education Inc, third edition, 2003.

[2] Ningrinla Marchang and Raja Datta. “Collaborative techniques for intrusion detection in mobile ad-hoc networks”,*Ad Hoc Networks*, 6(4): pp 508–523, 2008.

[3] C. Siva Ram Murthy and B. S. Manoj. “Ad Hoc Wireless Networks: Architectures And protocols”. Pearson Education India, 2008.

[4] Farooq Anjum, Dhanant Subhadra bandhu and Saswati Sarkar "Signature based Intrusion Detection for Wireless Ad-Hoc Networks: A Comparative Study of Various Routing Protocols”, 2003.

[5] Dorothy E. Denning "An Intrusion-detection Model” IEEE Transaction on Software Engineering, **13**, Vol.No. 7, Pp 222- 232, Feb 1987.

[6] Yu Liu, Yang Li and Hong Man, ”MAC Layer Anomaly Detection in Ad Hoc Networks”, Proceedings of the 6th IEEE Information Assurance Workshop,, pp. 402-409, June ,17, 2005.

[7] Yi an Huang and Wenke Lee. “A cooperative intrusion detection system for ad hoc networks” In *SASN*, pp. 135–147, 2003.

[8] “Cooperative Routing in Mobile Ad-hoc Networks: Current Efforts Against Malice and Selfishness.” By Sonja Buchegger, Jean-Yves Le Boudec. Proceedings of Mobile Internet Workshop. Informatik 2002., Dortmund, Germany, October 2002

[9] Yongguang Zhang and Wenke Lee. “Intrusion detection in wireless ad-hoc networks”. In *MOBICOM*, pp 275–283, 2000.

[10] J Yick, B Mukherjee… -“Computer networks”, 2008 – Elsevier

[11] S. Marti, T.J. Giuli, K. Lai and M. Baker, “Mitigating Routing Misbehaviour in Mobile Ad hoc Networks”, In Proc. ACM/IEEE Int’l Conf. on Mobile Computing and Networking, pp. 255-265, 2000.

[12] H.–Y. Chang, S.F. Wu and Y.F. Jou, “Real-Time Protocol Analysis for Detecting Link-State Routing Protocol Attacks”, ACM Tran. Inf. Sys.Sec., **1**, pp. 1-36, 2001.

[13] B. Sun, K. Wu, and U. Pooch. “Zone-based Intrusion Detection for Mobile Ad hoc Networks”, 2003.

[14] Tiranuch Anantvalee and Jie Wu “A Survey on Intrusion Detection in Mobile Ad Hoc Networks”, 2006, pp 170-196.

[15] Mobile ad hoc network. http ://en:wikipedia:org/wiki/Mobile_ad_hoc_network.

[16] O. Kachirski and R. Guha, “Effective Intrusion Detection using Multiple Sensors in Wireless Ad hoc Networks”, In Proc. 36th Annual Hawaii Int’l. Conf. on System Sciences (HICSS’03), pp.57.1, 2003.

[17] D. Sterne1, P. Balasubramanyam2, D. Carman1, B. Wilson1, R. Talpade3, C. Ko1,R. Balupari1, C-Y.Tseng2, T. Bowen3, K. Levitt2 and J. Rowe2 "A General Cooperative Intrusion Detection Architecture for MANETs”, 2006.

[18] Ioanna Stamouli, Patroklos G. Argyroudis, and Hitesh Tewari "Real-time Intrusion Detection for Ad hoc Networks” Proceedings of the Sixth IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks (WoWMoM’05), 0-7695-2342-0/05 $20.00 © 2005 IEEE.

[19] A. Karygiannis, E. Antonakakis, and A. Apostolopoulos “Detecting Critical Nodes for MANET Intrusion Detection Systems”, pp 7-15 , 2006.

[20] Xia Wang” Intrusion Detection Techniques in Wireless Ad Hoc Networks”vol.2,September 2006.

[21] R. Ranjana and M.Rajaram, “Detecting Intrusion Attacks in Ad-hoc Networks,” Asian Journal in Information Technology, **6(7)**, pp 758-761, 2007, ISSN: 1682:3915, Macdwell Journal 2007.

[22] Sheenu Sharma and Roopam Gupta. Simulation study of blackhole attack in the mobile ad hoc networks. In Journal of Engineering Science and Technology, pp 243–250, 2009.

[23] A.Rajaram and Dr. S. Palaniswami. Malicious node detection system for mobile ad hoc networks. (IJCSIT) International Journal of Computer Science and Information Technologies, 1(2): pp 77–85, 2010.

[24] Md. Safiqul Islam and Syed AshiqurRahman. “Anomaly Intrusion Detection System in Wireless Sensor Networks:Security Threats and Existing Approaches”. International Journal of Advanced Science and Technology Vol. 36, November, 2011.

Shaankar sharan Tripathi, B.E., M.E.(Pursuing) in Computer Technology & Application from Shri Shankaracharya College of Engineering & Technology, bhilai.India. , research areas are Wireless Computer Network, MANET & its Enhansement.

Prof. Sonu Agrawal,M.Tech (Gold Medalist) degree in Computer Technology from National Institute of Technology (NIT) Raipur, India in 2008.Currently pursuing Ph.D. from CSVTU, Bhilai. Having seven years long experience in the field of teaching.research areas are Wireless Computer Network, MANET, Bluetooth Network and its Enhansement, His research work has been published in many national and international journals.