Computer Engineering and Intelligent Systems
ISSN 2222-1719 (Paper) ISSN 2222-2863 (Online)
Vol.6, No.12, 2015

A Survey of Security Challenges and Issues in Manet

Sachin Gour[1] Prof. Sumit Sharma[2]
1.PG scholar, CSE, VIST, Bhopal, INDIA
2.HOD, CSE department , VIST, Bhopal, INDIA

Abstract
Nodes intriguing element in Mobile Ad-hoc Networks (MANET) are predictable to hold to the rules stated by the routing protocol utilized in the network. Safe routing protocols endeavor to decrease the ill-effect of nodes under the control of malicious entities who intentionally violate the protocol.. There are so many generic tools which are universal for individual as well as organizations for customers to offer protection which comprises Antivirus, Ant spam, etc., and network securities have turn into important issue in MANET. Security is one of the major issues in the MANET particularly w.r.t. complexity and size of the network. The main focus of this survey is to discuss & represent special characteristics of security in MANET and also apply several of the solutions security threats within MANET network similar to intruder activities, tapping and integrity, MANET link layer and network layer operations w.r.t. information security etc) w.r.t. MANET network. This Survey paper also discusses different number of security scenarios of MANET, Attacks in MANET and IDS in MANET.
Keywords: AODV, MANET, Network Security, IDS, Attacks

1. Introduction

The Wireless Local Area Networks (WLANs), developed back in the 1990s, are one of the most important license-exempt access network technologies nowadays. They allow data, voice and video communications over a wireless channel. A particular class of standards which has clearly dominated the market is the Institute of Electrical and Electronics Engineers (IEEE - 802.11) wireless LAN, also known as Wireless-Fidelity (Wi-Fi). These networks could operate in two modes; (i) infrastructure, which uses a wireless access point, and (ii) ad-hoc mode, which allows the creation of a self-configuring network consisting of mobile routers (for example laptops, smart phones) which are interconnected by wireless links. The latter are called MANETs [1] and their scope is to enable routing functionalities into the mobile nodes. A MANET, as described by the Internet Engineering Task Force (IETF) MANET Working Group (WG), is a temporary or permanent autonomous network comprised of free roaming nodes intending to establish wireless communications in absence of network infrastructures.

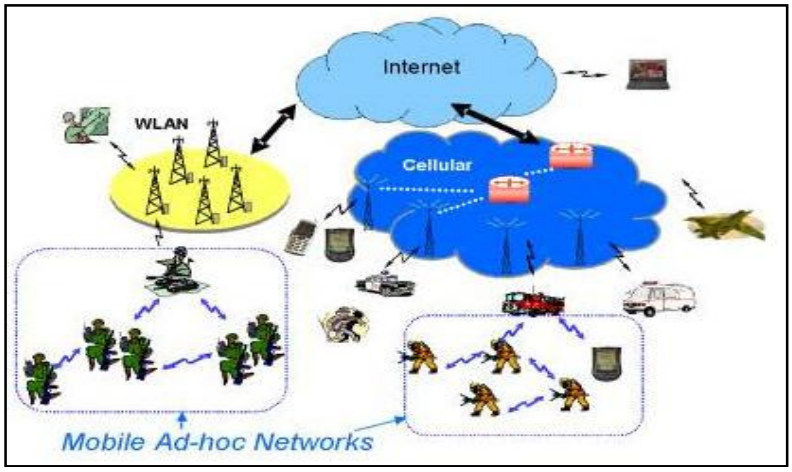

Fig.1: MANET Concept

The main role of MANETs is to enable wireless and mobile communication services without using the expensive service-provider network and without having a previously set up infrastructure. The network in that case is decentralized and the mobile nodes must accomplish network activities (network discovery) and must deliver the messages to each other by acting as routers. Therefore, MANET devices are able to sense the presence of other devices, establish communication links among them and communicate information. Concept of MANET is shown in fig.1:

It is also true that security has long been an active research topic in wire-line networks; but due to unique characteristics of MANET there are many challenges because of its self organizing behavior. These challenges are shared wireless medium, highly dynamic network topology, stringent resource constraints and open network architecture. It's true that existing security solutions for wired networks do not directly apply to the Mobile Ad-hoc Networks domain. MANET has so many objections w.r.t. wireless defense due to several of the following rationales:

1. The wireless network particularly responsible to attacks because of active eavesdropping to passive intrusive.
2. Due to less faith in Third Party attaches, it is extremely difficult to organize or apply security systems.
3. Generally Mobile gadgets have bounded calculation capacity and energy utilization functionalities which are weaker to Denial of Service (DoS) attacks. It is also unable to run intense security algorithms which require lots of computations such as public key algorithms.
4. Some of MANET's characteristics such as infrastructure less and self-organizing, there are extra probability for Faithfull node to be compromised and open attacks on networks..
5. It is complicated to differentiate between old routing and forged routing information because of node movement method. In node movement method it implements regular networking reconfiguration which generates more probability for attacks.

Mobile Ad-hoc Networks is a kind of infrastructure less, self-organizing, and the most important multi-hop network. By cause of its distributed and wireless environment there is an immense threat for system security inventors. Recently security complications in Mobile Ad-hoc Networks have adhere much consideration; the majority of the research attempts focusing on precise security regions, like securing routing protocols or establishing trust infrastructure or intrusion detection and response.

One of the main characteristic of MANET's w.r.t. security scheme opinion is the less clear line protection. In case of wired networks we have dedicated routers; which perform routing functionalities for devices however in case of MANETs are bothered every mobile node operates as a router and forward packets for other nodes. It is also true that the network channel is reachable equally to attackers as well as to network users. There is no finely described protocol or position where traffic from various nodes should be observed or entrance manages mechanism could be imposed. As a result of this there is no any protection method that divides internal network from the external network. As this mode the existing Mobile Ad-hoc Networks routing protocols, like Ad Hoc On Demand Distance Vector (AODV) [3] and Dynamic Source Routing (DSR) [2], and wireless MAC protocols, such as 802.11 [4], usually assumed to be trusted. As a result, an attacker could become a router and disrupt network operations.

There are generally three major security services for Mobile Ad-hoc Networks: Authentication, confidentiality, integrity.

- Authentication means accurate individuality is recognized to communicating authority.
- Confidentiality means communication information is reserved safe from illegal access.
- Integrity means communication is unchanged throughout the communication between two parties.

Amongst all these security services, authentication is perhaps the most significant and difficult matter in Mobile Ad-hoc Networks since it is the bootstrap of the entire security scheme. Once authentication is attained in Mobile Ad-hoc Networks then confidentiality is just an issue of encrypting algorithm on the session by utilizing keys. These security schemes could be offered individually or in grouping, it only based on demands.

Rest of the paper is organized as follow: section 2 explains about the existing routing protocols in MANET, In section 3 we describes different attacks of MANET, section 4 contains Intrusion detection system for MANET and finally we conclude our paper in section 5.

2. Routing In MANET

The MANET Working Group (WG) of the Internet Engineering Task Force (IETF), formed in 1997, is currently leading the standardization activities for an appropriate Internet Protocol (IP) based routing protocol functionality for both static and dynamic wireless routing topologies. The establishment of the MANET WG has been a catalyst towards research in the field of MANET routing, sparkling the creation of several scientific forums and the publication of vast amount of scientific papers addressing related challenges and possible solutions. The protocols developed by the MANET WG are considered to be the most suitable routing approaches for implementation. In addition to well-known wireless networking problems, MANETs present researchers with several peculiar routing challenges as described in [5, 6, and 7]. Fig.2 represents routing protocols in MANET.

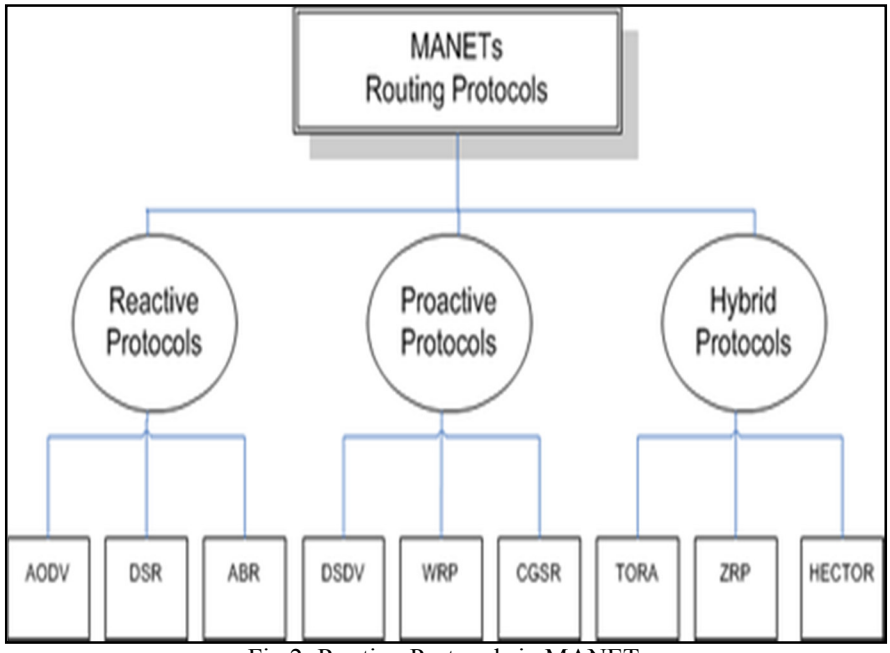

Fig.2: Routing Protocols in MANET

There are three main MANET routing approaches as follows

- Proactive MANET routing: The proactive routing approach, also known as table driven routing, consists of maintaining consistent and updated route information between all possible Source-Destination (S-D) pairs in the routing tables. Thus, routes between S-D pairs are always available reducing the latency in route establishment. Since a large amount of routing information is periodically disseminated and stored, the downside to such an approach is the high overhead of control packets and power consumption even when no data is being transmitted. Optimized Link State Routing (OLSR) [8] is a very popular proactive protocol, and in fact it is used for most of the implementations currently considered by IETF.
- Reactive MANET routing: A reactive routing approach, also known as on-demand routing, establishes and maintains routes between S-D pairs when requested by the data source node. Although such an approach generates routing overhead only on-demand, it nevertheless requires added latency for route discovery before routes are established. The Dynamic Source Routing Protocol (DSR) [2] is a well-known reactive protocol that utilizes route discovery and route maintenance on-demand to route data from a source to a destination. The AODV (Ad hoc On-Demand Distance Vector) routing protocol [3] is another well-known reactive protocol. AODV uses an on-demand route discovery and maintenance algorithm for route establishment in unicast routing and it is based on a modified Bellman-Ford [9] algorithm. AODV attempts to improve DSR by maintaining routing tables at the nodes, thus data packets do not have to contain routes. Another reactive MANET routing protocol is the AOMDV (Ad-hoc On-Demand Multipath Distance Vector) [10]. The main property which distinguishes AOMDV from AODV is that it enables loop-free and mutually link-disjoint multiple paths to a destination of a communication path providing fault tolerance. AOMDV chooses an optimal path until this breaks. Alternative routes are cached and they will be called only when a link failure occurs.
- Hybrid MANET routing: Hybrid MANET routing protocols use both reactive and proactive routing methods. There is also another classification of such routing protocols based on their zonal and converged characteristics. In zonal routing approaches, both reactive and proactive routing functionalities are used in different demarcated network areas. In converged approaches adaptively mechanisms are required to change protocol operation from reactive to proactive and vice versa. A novel MANET routing protocol called ChaMeLeon (CML) [11] is an adaptive hybrid routing approach that differs from previous protocols in that it does not maintain routing zones. Alternatively, CML operates in a converged approach that is optimally maintained using three phases of operation (Oscillation (O)-phase, Proactive (P)-phase and Reactive (R)-phase) while each phase has amplified features on top of the utilized flat routing mechanism that works in parallel to the traditional routing protocol.

3. Attacks in MANET

There are generally two protocols are used in Mobile Ad-hoc Networks, first is Link layer protocol that are used to supply connectivity among distinct mobile nodes in order to confirm one-hop connectivity by utilizing multihop wireless channels. Alternatively if node likes to expand connectivity to distinct multiple hops then MANET utilizes

network layer protocols. Second is a distributed protocol. In the coordination procedure distributed protocols classically suppose that every mobile node are cooperating w.r.t. communication but in reality this hypothesis is not achievable in hostile mobile networks situation since support is not imposed in MANET. The query occurs why? The simple cause is since malicious attackers disrupt protocol specification in order to disrupt network operations.

A. Classification of Network Layer Attacks

Network layer attacks could be classified in two major group, first is passive attacks and second is active attacks, as presented below in Figure 3

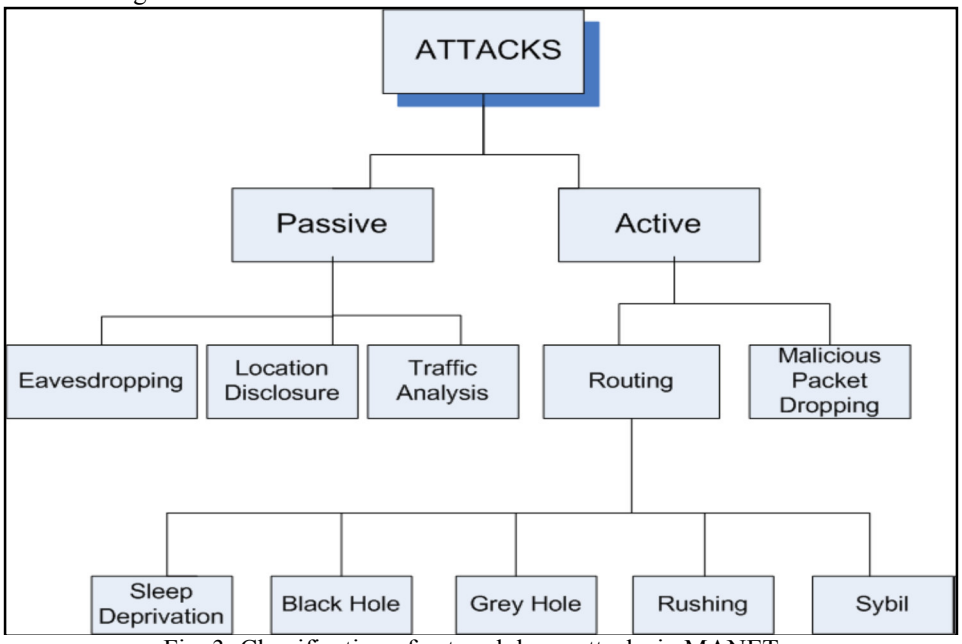

Fig. 3: Classification of network layer attacks in MANETs.

1) Passive Attacks: in Passive attacks the attacker doesn't disrupt the function of the routing protocol but tries to search important information's during the traffic analysis. This leads to the revelation of significant information of the network or nodes like the network topology, the identity of main nodes or the position of nodes. A few examples of passive attacks are given below:

Eavesdropping

Since the wireless connections are there in MANETs, any message posted by any node could be listened by all nodes equipped with a transceiver and inside the network, and if there is no any encryption is utilized then the attacker could obtain valuable information posted by sender node. The sender node and receiver node typically not aware about this type of attack has been happened. Even though in the majority cases eavesdropping are not measured to be as a severe attack, it could give very important information in several situations and then analyst have to be target on reducing it. Authors in [12] examined the danger of eavesdropping as a function of the broadcast range of the nodes and their geographical allocations.

Traffic Analysis and Location Disclosure

Attackers could eavesdrop to the traffic on wireless connections to determine the position of objective nodes by evaluating the message prototype, the features of the broadcasting and the quantity of information broadcasted by the nodes. For instance, in an arena situation, a huge number of network traffic usually streams to and from the control center. Traffic prototype study therefore permits an intruder to determine the commanding nodes in the MANETs. Though the information in a communication is protected by encryption, traffic evaluation could still be achieved to remove some valuable information. Even though passive attacks don't directly influence the network' functionality, in several MANET application developments, such as military communication etc., significant information discovery during traffic evaluation or simply eavesdropping could verify expensive. Examples of effort on evaluation and defense against these attacks could be established in [12] [13].

2) Active Attacks: In active attacks, intruders begin intrusive actions such as modifying, fabricating, injecting, forging or dropping information or routing packets, resulting in different disturbances to the network. A few of these attacks are reasoned by a solo action of an intruder and others could be reasoned by a series of actions by colluding intruders.

Active attacks bother the procedures of the network and could be so severe that they could bring down the whole network or disgrace the network performance significantly, in denial of service (DoS) attacks. Therefore, authors have focused on active network layer attacks. Active attacks can be more classified into malicious packet

dropping attacks and routing attacks, as mentioned in Figure 3.

Malicious Packet Dropping

A path among a source node and a destination node in Mobile Ad-hoc Networks is established utilizing a route discovery procedure. Once this has been finished, the source node starts sending the information packet to the neighbor node along the path; this midway node identifies the next hop node towards the target along the established path and forwards the information packet to it. This procedure continues until the information packet reaches the destination node. To achieve the needed operation of a MANET, it is significant that intermediate nodes forward information packets for any and every source nodes. However, a malicious node may choose to drop these packets instead of forwarding them; this is recognized as an information packet dropping attack, or data forwarding misbehavior.

In comparison to deliberately malicious behavior, in some cases nodes are unable to forward data packets because they are overloaded or have low battery reserves; alternatively the nodes may be selfish, for example saving their battery in order to process their own operations. Packet dropping attacks differ from black hole and grey hole attacks (see below) because there is no attempt to "capture" the routes in the network.

Routing Attacks

Both the reactive and proactive routing protocols are vulnerable to routing attacks because they route based on the assumption that all nodes cooperate to find the best path. Consequently, a malicious node could exploit the vulnerabilities of the cooperative routing algorithms and the lack of centralized control to launch routing attacks. In particular, the on-demand (reactive) MANET routing protocols, such as AODV [3] and DSR [2], allow intruders to launch a wide variety of attacks.

In the following we give examples of how different intrusive activities could cause various attacks in MANETs, illustrating them with AODV as the routing protocol.

Sleep Deprivation Attack

Sleep deprivation (SD) [14] is a distributed denial of service attack in which an attacker interacts with the node in a manner that appears to be legitimate, but where the purpose of the interaction is to keep the victim node out of its power-conserving sleep mode. In [15] the authors consider an intruder that could cause SD of a node by exploiting the vulnerability of the route discovery process of the protocol through malicious route request (RREQ) flooding in the following ways:

- Malicious RREQ Flooding 1: an intruder broadcasts a RREQ with a destination IP address that is within the network address range but there the corresponding node does not exist. This compels all the nodes to forward this RREQ because no one will have the route for this destination IP address.
- Malicious RREQ Flooding 2: After broadcasting a RREQ an intruder does not wait for the ring traversal time, but it continues resending the RREQ for the same destination with higher TTL values. This is a significant denial of service attack when we consider the energy constrained operations of MANETs.

Black Hole Attack

Intruders could exploit the vulnerability in route discovery procedures of on-demand routing protocols, such as AODV and DSR, when a node requires a route towards the destination.

The node sends a RREQ and an intruder advertises itself as having the fresh route. By repeating this for route requests received from other nodes, the intruder may succeed in becoming part of many routes in the network. The intruder, once chosen as an intermediate node, drops the packets instead of forwarding or processing them, causing a black hole (BH) [16] in the network. The way the intruder initiates the black hole attack and captures the routes may vary in different routing protocols. For example, in AODV, the destination sequence number (dest_seq) is used to represent the freshness of the route. A higher value of dest_seq means a fresher route. On receiving a RREQ, an intruder could advertise itself as having the fresher route by sending a Route Reply (RREP) packet with a new dest_seq number larger than the current dest_seq number. In this way, the intruder becomes part of the route to that destination. The severity of the attack depends on the number of routes in the network the intruder successfully becomes part of.

Grey Hole Attack

A grey hole attack (GH) [17] is a special case of the BH attack, in which an intruder first captures the routes, i.e. becomes part of the routes in the network (as with the BH attack), and then drops packets selectively. For example, the intruder may drop packets from specific source nodes, or it may drop packets probabilistically or drop packets in some other specific pattern. As we noted above, BH and GH attacks are different in nature from packet dropping attacks, where the attacker simply fails to forward packets for some reason. BH and GH attacks on the other hand comprise two tasks: the attacker first captures routes and then either drops all packets "BH attack" or some packets "GH attack"

Rushing Attack

In order to limit the control packet overhead, an on-demand protocol only requires nodes to forward the first RREQ that arrives for each route discovery. An attacker could exploit this property by spreading RREQ packets quickly throughout the network to suppress any later legitimate RREQ packets. For example, in AODV an intruder could

forge and forward a rushed RREQ, assigning a higher source sequence (src_seq) number to it; the intruder will also transmit the packet earlier than specified in the AODV protocol (this is the sense in which it is a "rushing" attack). This causes any later legitimate RREQ to be suppressed, and increases the probability that routes that include the intruder will be discovered instead of other valid routes. In [18] first described the rushing attack, and proposed its prevention through a set of generic mechanisms such as secure neighbor detection, secure route delegation and randomized RREQ forwarding.

Sybil Attack

Each node in a MANET requires a unique address to participate in routing, through which nodes are identified. However, in a MANET there is no central authority to verify these identities. An attacker could exploit this property and send control packets, for example RREQ or RREP, using different identities; this is known as a sybil attack (SY) [19]. This is an impersonation attack where the intruder could use either random identities or the identity of another node to create confusion in the routing process, or to establish bases for some other severe attack.

In summary, we note that the motivation of intruders behind launching either packet dropping or routing attacks is to achieve a certain goal such as denial of service (i.e. making certain resources or services, such as applications, web access, printing, or routing, unavailable to the intended users). In addition, other goals of intruders might include partitioning the network, creating routing loops, discovering valuable information, or theft of resources.

4. IDS for MANET

Their self-configuring nature, open medium and lack of centralized control make MANETs vulnerable to a wide range of attacks. Encryption, authentication and other standard security techniques couldn't provide full protection for MANETs. Therefore, intrusion detection mechanisms are highly recommended for these networks [20]. It is very crucial for the security of MANETs to have proactive defense mechanisms that could identify any anomalies before they could disrupt network operations. Conventional intrusion detection systems are designed for wired networks and couldn't be directly applied to their wireless equivalents [21] [22]. The short comings of fixed intrusion detection systems are obvious because they require centralized entities to control the operations of monitoring, detection and reporting. MANETs by nature are deployed where no fixed infrastructure is required, thus making it unreasonable to expect centralized systems to be effective in such networks.

With the wide-spread of mobile ad-hoc networks and their applications, it has become necessary to adapt to new dynamic security systems [23]. In the absence of a centralized authority for routing and monitoring, each node in the network acts as a host and a router. This makes MANETs highly susceptible to a wide range of attacks. These attacks could exploit the cooperative behavior of MANETs for their advantage [24]. Compromising a single node in the network could jeopardize the security of the whole network.

Current IDS architectures for MANETs are divided into three main categories according to their implementation. These three types are: host-based IDS, distributed IDS and mobile agents IDS [25]. In host-based intrusion detection the IDS is deployed on each host (node) locally. Whereas in distributed IDS the functionality of the IDS is distributed among nodes where each node has a specific task or tasks. The third type use mobile agents that roam among nodes to detect and report anomalies.

Host Based IDS

Shakshuki et.al [26] proposed local IDS named Enhanced Adaptive Acknowledgment (EAACK) for MANETs. Their solution addresses some of the weaknesses of the Watchdog scheme, namely, false misbehavior, limited transmission power, and receiver collision. The IDS prevents attackers from initiating forged acknowledgment attacks by incorporating digital signature in every message. This proposal is based on the acknowledgment scheme in which the destination node (D) is required to send an acknowledgment packet back to the source node (S).

To overcome the risk of attackers sending forged acknowledgment packets the authors proposed the use of digital signatures. All acknowledgment packets are digitally signed before they are sent out to be verified by the destination. The model also implements a mechanism to discover when a misbehavior report is initiated by an attacker to damage the operation of the network. When a node receives a report that another node is misbehaving it runs a verification scheme to confirm the report by sending a message to that node through an alternative route. One of the drawbacks in this solution is: it requires cryptographic keys to be distributed in advance but it does not propose any key exchange method. Another disadvantage is the fact that digital signatures introduce large network overhead which could be reduced using other cryptographic techniques.

Distributed IDS

Paramasiva and Pitchai [27] introduced a novel intrusion detection system that uses a game-theory based model to detect malicious nodes in the network. The authors used the Bayesian game concept to model the interaction between neighboring nodes of MANETs. In their paper, they described the interaction between a regular and malicious node as a 2 player dynamic non-cooperative game. Each mobile node is capable of monitoring, detecting and generating alarms in the case of an attack. The attack database and signatures are locally stored in each node along with system audit data, normal application profiles, and IDS logs. The network is divided into clusters and

a cluster head is elected through a clustering algorithm. The cluster head is responsible of updating normal behavior profile and attack signatures. The cluster head could also patch and install programs, analyze and diagnose anomalous nodes, and assess the local IDS running on other nodes in the cluster.

If an intrusion is detected, the cluster head is notified by the decision making unit to make further diagnosis and analysis on that specific node. A prober action is taken and the compromised node is advertised across the network if and when the cluster head confirms the attack. This model promises to reduce the overhead introduced by running all the IDS functions on each single node. However, this proposal makes the assumption that one node is attacked at a time and that collusions between malicious nodes do not occur. The model also increases the power, and processing requirement on each node.

IDS with mobile agents

Stafrace and Antonopoulosb [28] proposed Mobile agents based IDS with military tactics for the detection of Sinkhole attacks in MANET [28]. The mobile agents are deigned to work as a tactical squad that conducts regular petrol missions through MANET nodes. Their approach is based on structured military command-base where agents get their instructions to police routes to detect any malicious activity. Some routes are patrolled more than others based on the a Sinkhole attack in (WSN) using the Ad-hoc On Demand Distance Vector (AODV) as routing protocol. Calculated risk The model was tested through simulation of a Sinkhole attack in (WSN) using the Ad-hoc On Demand Distance Vector (AODV) as routing protocol.

5. CONCLUSION

MANETs are gaining more and more solid ground in wireless communications. As the applications increase rapidly, threats and security issues also increase. In a wireless environment, security is a vital building block. Insecure wireless networks, are simply unusable. In this paper, we have introduced a short review of the most common threats and attacks. Mitigation techniques of the threats were also discussed. A few common types of attacks on MANET along with three different classifications of attacks on MANET security were presented. Attacks were discussed in the scope of these classifications along with their counter-measures.

The characteristics of MANET make it a target for types of attacks that are not possible on other types of wired and/or wireless networks. For example, having constrained battery life makes its vulnerable to battery-draining attacks like DoS. Also, being a wireless network makes it inherently vulnerable to jamming attacks that could render the complete wireless network unusable. Attacks aimed at the routing process have proved to be effective in disturbing the network operation. Attacks like wormhole, tunneling, and DoS have proved their effectiveness against almost all MANET routing protocols.

Active attacks are considered more dangerous as they disrupt the proper operation of the MANET. While passive attacks are not necessarily harmful as standalone attacks, they could be used as a first step to more serious and harmful attacks like blackhole attacks. Thus, passive attacks should not be overlooked or ignored.

Research in MANET security is diversified as the sources of threats are diversified. A good direction in research would be the creation of a trust-based system in which the type and diversity of security techniques applied rely on the level of trust. Although some research was done in this direction, specifically in terms of routing protocols, it is still a fresh area with high potential.

References

[1] Basagni, Stefano, Marco Conti, Silvia Giordano, and Ivan Stojmenovic, eds.Mobile ad hoc networking. John Wiley & Sons, 2004.
[2] Johnson, David B., and David A. Maltz. "Dynamic source routing in ad hoc wireless networks." In Mobile computing, pp. 153-181. Springer US, 1996.
[3] Perkins, Charles, Elizabeth Belding-Royer, and Samir Das. Ad hoc on-demand distance vector (AODV) routing. No. RFC 3561. 2003.
[4] IEEE Computer Society LAN MAN Standards Committee. "Wireless LAN medium access control (MAC) and physical layer (PHY) specifications." (1997).
[5] Macker, Joseph. "Mobile ad hoc networking (MANET): Routing protocol performance issues and evaluation considerations." (1999).
[6] Burbank, Jack L., Philip F. Chimento, Brian K. Haberman, and William T. Kasch. "Key challenges of military tactical networking and the elusive promise of MANET technology." Communications Magazine, IEEE 44, no. 11 (2006): 39-45.
[7] Conti, Marco, and Silvia Giordano. "Multihop ad hoc networking: The reality."Communications Magazine, IEEE 45, no. 4 (2007): 88-95.
[8] Clausen, Thomas, and Philippe Jacquet. Optimized link state routing protocol (OLSR). No. RFC 3626. 2003.
[9] T. Cormen, H. Leiserson, E. Charles, and R. Ronald, “The bellman-ford algorithm,” MIT Press and McGraw-Hill, pp. 651–655, 2009.
[10] Marina, Mahesh K., and Samir R. Das. "On-demand multipath distance vector routing in ad hoc networks."

In Network Protocols, 2001. Ninth International Conference on, pp. 14-23. IEEE, 2001.
[11] Ramrekha, Tipu Arvind, and Christos Politis. "A hybrid adaptive routing protocol for extreme emergency ad hoc communication." In Computer Communications and Networks (ICCCN), 2010 Proceedings of 19th International Conference on, pp. 1-6. IEEE, 2010.
[12] Kao, Jung-Chun, and Radu Marculescu. "Eavesdropping minimization via transmission power control in Ad-Hoc wireless networks." In Sensor and Ad Hoc Communications and Networks, 2006. SECON'06. 2006 3rd Annual IEEE Communications Society on, vol. 2, pp. 707-714. IEEE, 2006.
[13] He, Ting, Ho Yin Wong, and Kang-Won Lee. "Traffic analysis in anonymous MANETs." In Military Communications Conference, 2008. MILCOM 2008. IEEE, pp. 1-7. IEEE, 2008.
[14] Pirretti, Matthew, Sencun Zhu, Narayanan Vijaykrishnan, Patrick McDaniel, Mahmut Kandemir, and Richard Brooks. "The sleep deprivation attack in sensor networks: Analysis and methods of defense." International Journal of Distributed Sensor Networks 2, no. 3 (2006): 267-287.
[15] Nadeem, Adnan, and Michael Howarth. "Adaptive intrusion detection & prevention of denial of service attacks in MANETs." In Proceedings of the 2009 International Conference on Wireless Communications and Mobile Computing: Connecting the World Wirelessly, pp. 926-930. ACM, 2009.
[16] Kurosawa, Satoshi, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto. "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method." IJ Network Security 5, no. 3 (2007): 338-346.
[17] Sen, Jaydip, M. Girish Chandra, S. G. Harihara, Harish Reddy, and P. Balamuralidhar. "A mechanism for detection of gray hole attack in mobile Ad Hoc networks." In Information, Communications & Signal Processing, 2007 6th International Conference on, pp. 1-5. IEEE, 2007.
[18] Hu, Yih-Chun, Adrian Perrig, and David B. Johnson. "Rushing attacks and defense in wireless ad hoc network routing protocols." In Proceedings of the 2nd ACM workshop on Wireless security, pp. 30-40. ACM, 2003.
[19] Piro, Chris, Clay Shields, and Brian Neil Levine. "Detecting the sybil attack in mobile ad hoc networks." In Securecomm and Workshops, 2006, pp. 1-11. IEEE, 2006.
[20] Pinnaka, A. K., D. Tharashasank, and V. S. K. Reddy. "Cost performance analysis of intrusion detection system in mobile wireless ad-hoc network." InAdvance Computing Conference (IACC), 2013 IEEE 3rd International, pp. 536-541. IEEE, 2013.
[21] Husain, Syed, S. C. Gupta, Mukesh Chand, and H. L. Mandoria. "A proposed model for Intrusion Detection System for mobile adhoc network." In Computer and Communication Technology (ICCCT), 2010 International Conference on, pp. 99-102. IEEE, 2010.
[22] Mafra, Paulo M., Joni da Silva Fraga, and Altair Olivo Santin. "A Distributed IDS for Ad Hoc Networks." In Advanced Information Networking and Applications Workshops (WAINA), 2012 26th International Conference on, pp. 478-483. IEEE, 2012.
[23] Lin, Hsiao-Ching, Ming-Kung Sun, Han-Wei Huang, Chin-Yang Henry Tseng, and Hui-Tang Lin. "A Specification-Based Intrusion Detection Model for Wireless Ad Hoc Networks." In Innovations in Bio-Inspired Computing and Applications (IBICA), 2012 Third International Conference on, pp. 252-257. IEEE, 2012.
[24] Selvamani, K., S. Anbuchelian, S. Kanimozhi, R. Elakkiya, S. Bose, and A. Kannan. "A hybrid framework of intrusion detection system for resource consumption based attacks in wireless ad-hoc networks." In Systems and informatics (ICSAI), 2012 international conference on, pp. 8-12. IEEE, 2012.
[25] Basagni, Stefano, Marco Conti, Silvia Giordano, and Ivan Stojmenovic, eds.Mobile Ad Hoc networking: the cutting edge directions. Vol. 35. John Wiley & Sons, 2013.
[26] SakilaAnnarasi, R., and S. Sivanesh. "A secure intrusion detection system for MANETs." In Advanced Communication Control and Computing Technologies (ICACCCT), 2014 International Conference on, pp. 1174-1178. IEEE, 2014.
[27] Paramasiva, B., and K. Mohaideen Pitchai. "Modeling intrusion detection in mobile ad hoc networks as a non cooperative game." In Pattern Recognition, Informatics and Mobile Engineering (PRIME), 2013 International Conference on, pp. 300-306. IEEE, 2013.
[28] Stafrace, Stefan K., and Nick Antonopoulos. "Military tactics in agent-based sinkhole attack detection for wireless ad hoc networks." Computer Communications 33, no. 5 (2010): 619-638.