Volume 3, Issue 7, July 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Review Report ATTACK Analysis in Mobile Ad HOC Network Based on System Observations

Nidhi Saxena[1], **Iyagpal Yadav** [2]
(Institute of Engineering and Science IPS Academy)
(Indore, Madhya Pradesh)

Vipul Saxena
Oriental Institute of Tech. & manag.
(Bhopal Madhya Pradesh, India)

Abstract:-The present work is dedicated to study attack and counter measure in MANET. After a short introduction what MANETs are and network security we present a survey of various attack in MANET pertaining to fill routing protocols. Our work and with a proposal analytical modeling to model some of these attack like cooperative Blackhole Attack, wormhole Attack, Selfish Attack, Sleep Deprivation, . We uses two different methods to observe the parameters of above attacks i.e. NEURAL NETWOR AND CLUSTERING and the simulation of these attacks is done by using a simulator network named OPNET MODULER 14.0.

Keywords: MANET, routing, security, modeling, simulation, clustering and neural network.

1. Introduction:

A mobile ad hoc network (MANET) is a dynamic wireless network that can be formed without any pre-existing infrastructure in which each node can act as a router. MANET has no clear line of defense, so, it is accessible to both legitimate network users and malicious attackers. In the presence of malicious nodes, one of the main challenges in MANET is to design the robust security solution that can protect MANET from various routing attacks. Particularly, we have examined and simulate the different routing attacks, such as Blackhole Attack, wormhole Attack, Selfish Attack, Sleep Deprivation, Normal Attack [1].The problem of the MANET is how to find the investment of lower costs in rated capacities and reserves which ensures the routing of the nominal traffic and guarantees its reliability in the event of any breakdown of arc or node. That's why several families routing protocols emerged. Each protocol can be classified as a reactive like AODV (Ad hoc On Demand Distance Vector) and DSR (Dynamic Source Routing), proactive like OLSR (Optimized Link State Protocol), or hybrid like ZRP (or Routing Protocol Zones) [2]. We are using OPNET for our research because of the several benefits it offers. OPNET provides a GUI for the topology design, which allows for realistic simulation of networks, and has a performance data collection and display module. Another advantage of using OPNET is that it has been used extensively and there is wide confidence in the validity of the results it produces. OPNET enables realistic analysis of performance measures and the effectiveness of intrusion detection techniques. In a similar work, OPNET was used in a performance study of an intrusion detection system using statistical preprocessing and neural network classification [3]. One of our research goals is to study techniques that can speed up OPNET simulation for large data files suspected of intrusion attacks.

2. Literature Review:

Although different detection approaches exist for threat in general terms all of them consist of the following basic modules or stages (Fig. 1)

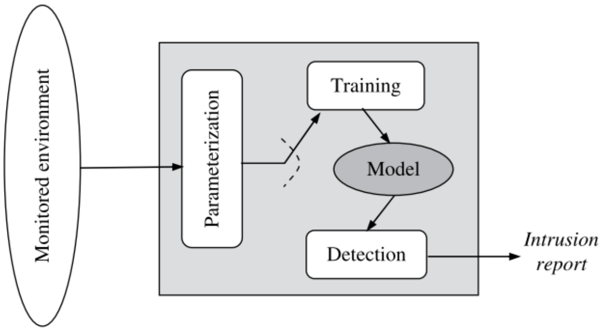

Figure 1. Basic functional architecture detection system.

Parameterization: In this stage, the observed instances of the target system are represented in a pre-established form. Training stage: The normal (or abnormal) behavior of the system is characterized and a corresponding model is built. This can be done in very different ways, automatically or manually.

Detection stage: Once the model for the system is available, it is compared and analyzed with the (parameterized) observed traffic. Detection techniques can be classified into three main categories (see Fig. 2): statistical-based, knowledge-based, and machine learning-based. In the statistical-based case, the behavior of the system is represented from a random viewpoint. On the other hand, knowledge-based techniques try to capture the claimed behavior from available system data (protocol specifications, network traffic instances, etc.). Finally, machine learning schemes are based on the establishment of an explicit or implicit model that allows the patterns analyzed to be categorized. Two key aspects concern the evaluation, and thus the comparison, of the performance of alternative intrusion detection approaches: these are the efficiency of the detection process, and the cost involved in the operation. Without underestimating the importance of the cost, at this point the efficiency aspect must be emphasized. Four situations exist in this context, corresponding to the relation between the result of the detection for an analyzed event (‘‘normal’’ vs. ’’attacked’’) and its actual nature (‘‘innocuous’’ vs. ‘‘malicious’’). These situations are: false positive (FP), if the analyzed event is innocuous (or ‘‘clean’’) from the perspective of security, but it is classified as malicious; true positive (TP), if the analyzed event is correctly classified as intrusion/malicious; false negative (FN), if the analyzed event is malicious but it is classified as normal/innocuous; and true negative (TN), if the analyzed event is correctly classified as normal/innocuous. It is clear that low FP and FN rates, together with high TP and TN rates, will result in good efficiency values [4].

The fundamentals for statistical, knowledge and machine learning-based, as well as the principal subtypes of each, are described below.

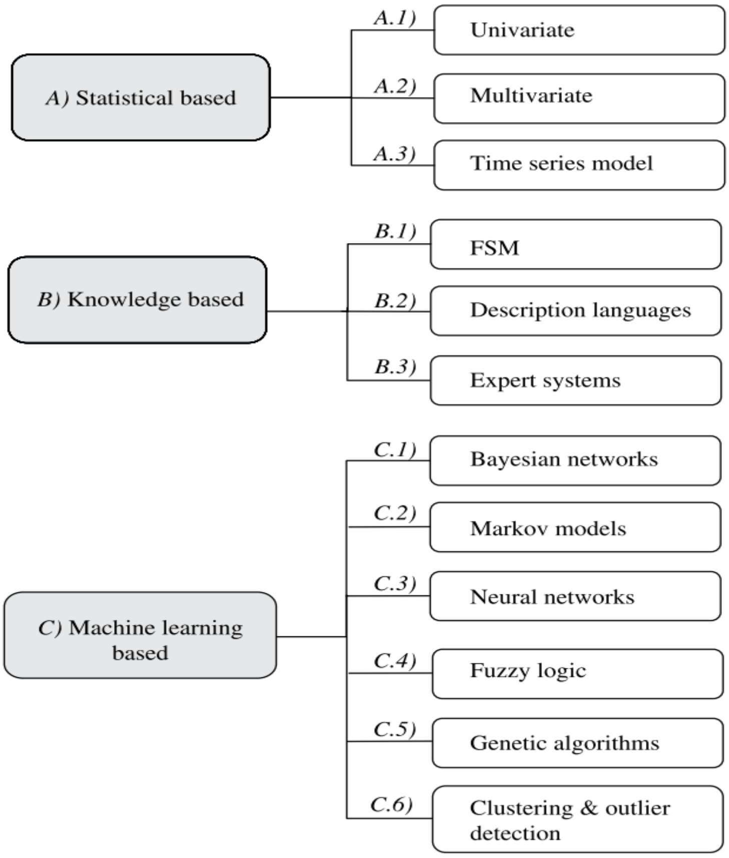

Figure 2. Classification of the anomaly detection techniques .

Expert system

These work on a previously defined set of rules describing an attack. All security related events incorporated in an audit trail are translated in terms of if-then-else rules. Examples are Wisdom & Sense and Computer Watch (developed at AT&T).

Signature analysis

Similarly to expert System approach, this method is based on the attack knowledge. They transform the semantic description of an attack into the appropriate audit trail format. Thus, attack signatures can be found in logs or input data streams in a straightforward way. An attack scenario can be described, for example, as a sequence of audit events that a given attack generates or patterns of searchable data that are captured in the audit trail. This method uses abstract equivalents of audit trail data. Detection is accomplished by using common text string matching mechanisms. Typically, it is a very powerful technique and as such very often employed in commercial systems (for example Stalker, Real Secure, NetRanger, Emerald eXpert-BSM).

State-transition analysis

Here, an attack is described with a set of goals and transitions that must be achieved by an intruder to compromise a system. Transitions are represented on state-transition diagrams.

Statistical analysis approach

This is a frequently used method (for example SECURENET). The user or system behavior (set of attributes) is measured by a number of variables over time. Examples of such variables are: user login, logout, number of files accessed in a period of time, usage of disk space, memory, CPU etc. The frequency of updating can vary from a few minutes to, for example, one month. The system stores mean values for each variable used for detecting exceeds that of a predefined threshold. Yet, this simple approach was unable to match a typical user behavior model. Approaches that relied on matching individual user profiles with aggregated group variables also failed to be efficient. Therefore, a more sophisticated model of user behavior has been developed using short- and long-term user profiles. These profiles are regularly updated to keep up with the changes in user behaviors. Statistical methods are often used in implementations of normal user behavior profile-based Intrusion Detection Systems.

Neural Networks

Neural networks use their learning algorithms to learn about the relationship between input and output vectors and to generalize them to extract new input/output relationships. With the neural network approach to intrusion detection, the main purpose is to learn the behavior of actors in the system (e.g., users, daemons). It is known that statistical methods partially equate neural networks. The advantage of using neural networks over statistics resides in having a simple way to express nonlinear relationships between variables, and in learning about relationships automatically. Experiments were carried out with neural network prediction of user behaviors. From the results it has been found that the behavior of UNIX super-users (*roots*) is predictable (because of very regular functioning of automatic system processes). With few exceptions, behavior of most other users is also predictable. Neural networks are still a computationally intensive technique, and are not widely used in the intrusion detection community.

User intention identification

This technique (that to our knowledge has only been used in the SECURENET project) models normal behavior of users by the set of high-level tasks they have to perform on the system (in relation to the users' functions). These tasks are taken as series of actions, which in turn are matched to the appropriate audit data. The analyzer keeps a set of tasks that are acceptable for each user.

Machine learning

This is an artificial intelligence technique that stores the user-input stream of commands in a vectorial form and is used as a reference of normal user behavior profile. Profiles are then grouped in a library of user commands having certain common characteristics [4].

Data mining

Generally refers to a set of techniques that use the process of extracting previously unknown but potentially useful data from large stores of data. Data mining method excels at processing large system logs (audit data). However they are less useful for stream analysis of network traffic. One of the fundamental data mining techniques used in intrusion detection is associated with *decision trees* [4]. Decision tree models allow one to detect anomalies in large databases. Another technique refers to segmentation, allowing extraction of patterns of unknown attacks [4]. This is done by matching patterns extracted from a simple audit set with those referred to warehoused unknown attacks [4]. A typical data mining technique is associated with finding *association rules*. It allows one to extract previously unknown knowledge on new attacks [4] or built on normal behavior patterns. Anomaly detection often generates false alarms. With data mining it is easy to correlate data related to alarms with mined audit data, thereby considerably reducing the rate of false alarms [4].

The detection of anomaly aims at distinguishing a new model like part of self or no-self, given a model of system of self [4]. Structured Gene Activation (SGA) is a type of evolutionary algorithm which incorporates the redundant genetic material, which is controlled by a mechanism. It uses the multi-layer genomic structures for its chromosome i.e. all the genetic material (expressed or not) "is structured" in a hierarchical chromosome. The activation and deactivates mechanism these coded genes. This solution is implemented in AODV [4]. A solution based on the reputation named Collaborative Reputation (CORE) and Cooperation Of Nodes and Fairness In Dynamic Ad-hoc Network (CONFIDANT) which consists in collecting information on an old behavior of the tested entity by others [4]. A solution based on the payment (Nuglets) which requires with nodes which benefit from the resources of the network (transmitters and/or receivers) to pay "service providers" (intermediate nodes)[4] and a solution based on the localization (directional antennas)

Routing protocols

Mobile Ad Hoc Network (MANET) is collection of multi-hop wireless mobile nodes that communicate with each other without centralized control or established infrastructure. The wireless links in this network are highly error prone and can go down frequently due to mobility of nodes, interference and less infrastructure. Therefore, routing in MANET is a critical task due to highly dynamic environment. In recent years, several routing protocols have been proposed for mobile ad hoc networks and prominent among them are DSR, AODV . This research paper provides an overview of these protocols by presenting their characteristics, functionality, benefits and limitations and then makes their comparative analysis so to analyze their performance. The objective is to make observations about how the performance of these protocols can be improved. There are various type of routing protocol. These are following *AODV, OLSR, DSR, ZRP*.[9].

AODV (Ad Hoc On Demand Distance Vector Routing Protocol)

it provide fast efficient route establishment between mobile nodes that need to communicate with each other. Since AODV has been specifically designed for Ad Hoc wireless network. In addition to unicast routing, AODV support multicast and broadcast as well. AODV can be extended to support Quality of Services (QoS). AODV is an on demand algorithm, which means that routes between nodes are built only when means they are requested by originator nodes. Routes are maintained only as long as originator need then.

OLSR (*Optimized Link State Routing Protocol*)

This protocol is based on link state algorithm and it is proactive (or table- driven) in nature. It employs periodic exchange of message to maintain topology information of the network at each node. OLSR is an optimization over a pure link state protocol as it compact the size of information sent in the message and furthermore reduces the number of retransmission to flood these messages in entire network. This protocol uses the multipoint broadcasting (relaying) tech to efficient and economically flood its control message.

DSR(Dynamic Source Routing)

DSR routing protocol, which are used fir efficient routing under different scenario in MANET, which play a critical role in place where wired network are neither available nor economical to deploy.

DSR allows the network to be complete self organization and self configure, without the need for any existing network infrastructure or administration. The protocol composed of two mechanism of route discovery and route maintain which work together to allow nodes to discover and maintain source route to arbitrary in the ad hoc network.[8]

ZRP (Zone Routing Protocol)

ZRP is a well known hybrid routing protocol that is most suitable for large scale network. The ZRP framework is designed to provide a balance between the contrasting proactive and reactive routing approaches. its name is derived from the use of one that define the transmission radius for every participating node

ZRP uses a proactive mechanism of node discovery within a node's immediate neighborhood, while interzone communication is carried out by using reactive approaches.[10]

Attacks in Routing Protocol of Mobile Ad Hoc Networks

An attack is an action which aims at compromising the security of the network. They are many and varied in these MANET.

Blackhole attack:

consists in dropping some routing messages that node receives [6,7,8]. It was declined in several particularity alternatives, having different objectives, among which we can quote:

Routing loop:-

which makes it possible for a node to create loops in the network;

Gray hole:-

which lets pass only the packages of routing and diverts the data;

Blackmail:-

which makes it possible for a node attacker to isolate another.

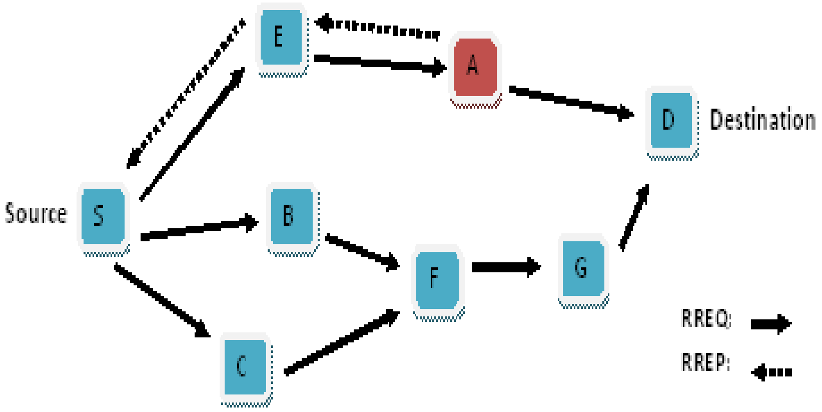

Figure 3: Blackhole attack

The selfish attack:

Consists in not collaborating for the good performance of the network. We can identify two types of nodes which do not wish to take part in the network. Defective nodes i.e. do not work perfectly. Those which are malevolent, it is those which intentionally, try to tackle the system: attack on the integrity of the data, the availability of the services, the authenticity of the entities (denial-of-service, interception of messages, usurpation of identity, etc). Selfish nodes are entities economically rational whose objective is to maximize their benefit. [6]

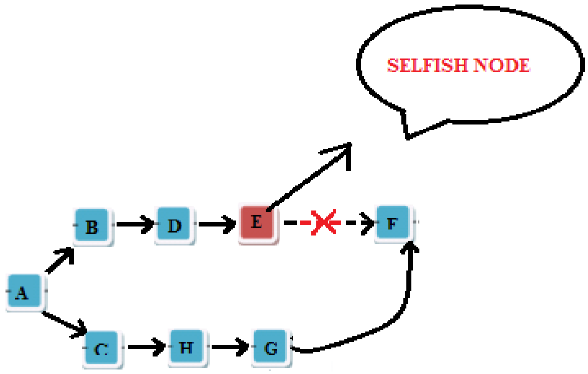

Figure 4: Selfish attack

Sleep deprivation attacks:

This kind of attack is actually more specific to the mobile ad hoc networks. The aim is to drain off limited resources in the mobile ad hoc nodes (e.g. the battery powers), by constantly makes them busy processing unnecessary packets. In a routing protocol, sleep deprivation attacks might be launched by flooding the targeted node with unnecessary routing packets. For instance, attackers could flood any node in the networks by sending a huge number of route request (RREQ), route replies (RREP) or route error (RERR) packets to the targeted node. As a result, that particular node is unable to participate in the routing mechanisms and rendered unreachable by the other nodes in the networks.[8]

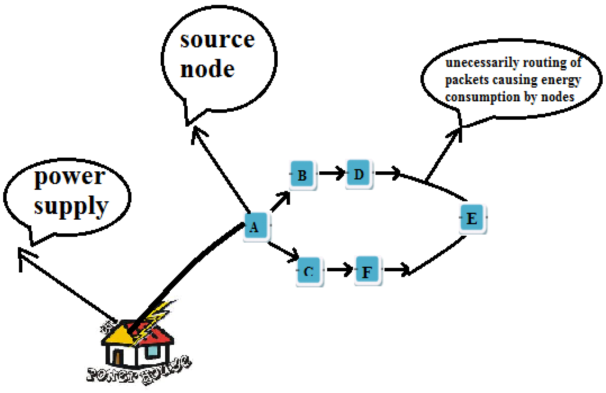
source node
unecessarily routing of packets causing energy consumption by nodes
power supply
A
B
D
E
C
F
power house

Figure 5: Sleep deprivation attack

Wormhole attack:

A wormhole attack [9] is one of the most sophisticated and severe attacks in MANETs. In this attack, a pair of colluding attackers record packets at one location and replay them at another location using a private high speed network. The seriousness of this attack is that it can be launched against all communications that provide authenticity and confidentiality. Figure shows an example of the wormhole attack against a reactive routing protocol. In the figure, we assume that nodes A1 and A2 are two colluding attackers and that node S is the target to be attacked.During the attack, when source node S broadcasts an RREQ to find a route to a destination node Figure : Wormhole attack on reactive routing

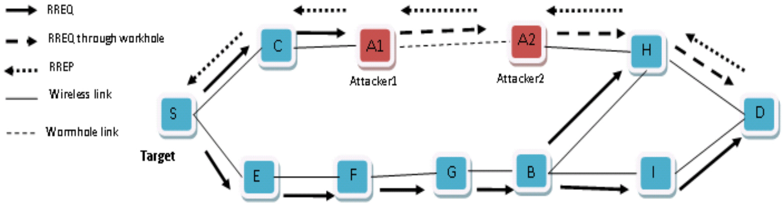

Figure 6: Wormhole attack

D, its neighbors C and E forward the RREQ as usual. However, node A1, which received the RREQ, forwarded by node C, records and tunnels the RREQ to its colluding partner A2.Then, node A2 rebroadcasts this RREQ to its neighbor H. Since this RREQ passed through a high-speed channel, this RREQ will reach node D first. Therefore, node D will choose route D-H-C-S to unicast an RREP to the source node S and ignore the same RREQ that arrived later. As a result, S will select route S-H-D that indeed passed through A1 and A2 to send its data.

Proposed Algorithm

Since there is no data available about the network characteristics on attacked situation, hence it is needed to simulate the network for such condition and to collect the data, for this purpose a network simulator (OPNET) is used here, and after simulating the network for different scenario the raw data is collected. Now this data is classified into different group based on the data type (delay, drop rate, conjunction, packet type, bandwidth utilization, process status, services running, and processor utilization), then each data set it normalized by detecting its maximum and minimum values by the following formula

$$V_{norm} = \frac{V - V_{min}}{V_{max} - V_{min}}$$

The normalized values set are arranged in an array to represent system condition by a vector this vector can be represented by

$$Trn_{vect} = [V_{norm1}, V_{norm2}, V_{norm3}, \ldots\ldots V_{normn}]$$

Hence the system states can be projected into a hyper space of n dimensions.

According to the system states, vectors of that states are grouped and the centre for thatgroup is calculated after that the maximum radius is also calculated (by measuring the distance from centre point to the point of maximum distance).

These processes provide the m centers for m different states (under attack, serious attack, ok etc.) of network and their maximum movement. Now for detecting the system status any time the system data is collected and converted in to the vector as stated above and then using the soft computing technique training and the alarm is generated for the nearest point from the present vector.

3. Conclusion:

The model of the attack detector for MANET presented in this paper is not only capable of attack situation but can also classifying the individual attacks. The Detection accuracy of the system will be excellent also the algorithm have very low FPR hence reduces the chances of false alarming. Further it could achieve much better performance by increasing the number of samples taken and increasing the number of characteristics parameter selected.

Reference

[1] *Rashid Hafeez Khokhar, Md Asri Ngadi, Satria Mandala Faculty of Computer Science and Information System Department of Computer System & Communication Universiti Teknologi Malaysia (UTM) Skudai, 81310, Johor Bahru, Malaysia.* ***A*** *Review of Current Routing Attacks inMobile Ad Hoc Networks.*

[2] *Shabana Razak, Mian Zhou, Sheau-Dong Lang* School of Electrical Engineering & Computer Science and National Center for Forensic Science* University of Central Florida, Orlando, FL 32816. Network Intrusion Simulation Using OPNET.*

[3] *Zheng Zhang, Jun Li, C.N. Manikopoulos, Jay Jorgenson, Jose Ucles, "HIDE: A Hierarchical Network Intrusion Detection System Using Statistical Preprocessing and Neural Network Classification", in Proceedings of 2001 IEEE Man Systems and Cybernetics Information Assurance Workshop, 2001.*

[4] *Anomaly-based network intrusion detection: Techniques, systems and challenges P. Garcı´a-Teodoroa,*, J. Dı´az-Verdejoa, G. Macia´-Ferna´ndeza, E. Va´zquezb aDepartment of Signal Theory, Telematics and Communications – Computer Science and Telecommunications Faculty, University of Granada, Granada, Spain bDepartment of Telematic Engineering - Universidad Polite´cnica de Madrid, Madrid, Spain.*

[5] *Dr Karim KONATE and Abdourahime GAYE Department of Mathematics and Computing University Cheikh Anta DIOP, Dakar A Proposal Mechanism Against the Attacks: Cooperative Blackhole, Blackmail, Overflow and Selfish in Routing Protocol of Mobile Ad Hoc Network.*

[6] *Curtmola Reza, Security of Routing Protocols in Ad Hoc Wireless Networks. 600.647 - Advanced Topics in Wireless Networks, February 2007, pages 26..*

[7] *Attacks against Mobile Ad Hoc Networks Routing Protocols S. A. Razak, S. M. Furnell, P. J. Brooke Network Research Group, University of Plymouth Plymouth, Devon PL4 8AA*

.[8] *Implementing and comparing DSR and DSDV routing protocols for mobile AD Hoc networking "Bikas Rathi "*

[9] Current Research Work on Routing Protocols for MANET: A Literature Survey G.Vijaya Kumar 1, Y.Vasudeva Reddyr 2, Dr.M.Nagendra 3 1 CSE Dept, Asst Prof,G.Pulla Reddy Engg.College(Autonomous),Kurnool-2,AP,India 3 MCA Dept, Asst Prof,G.Pulla Reddy Engg.College(Autonomous),Kurnool-2,AP,India 3 CS&T Dept, Assoc Prof, SKU, Anantapur, AP, India

[10] Zone Routing Protocol (ZRP) Nicklas Beijar Networking Laboratory, Helsinki University of Technology P.O. Box 3000, FIN-02015 HUT, Finland Nicklas.Beijar@hut.fi