Intrusion Detection System for Wireless ADHOC Network using Time Series Techniques

M. Ashikur Rahman
Lecturer
Department of Computer Science and Engineering,
University of South Asia,
Bangladesh

Sabbir M. Saleh
Lecturer
Department of Computer Science and Engineering,
University of South Asia,
Bangladesh

Syed Maruful Huq
Lecturer
Department of Computer Science and Engineering,
University of South Asia,
Bangladesh

ABSTRACT

Computer security and intrusion detection has developed into progressively more significant in recent computer sector, which is providing security of confidential data and information. At present, different progress and advances of intrusion detection is applying and operating, although in consequence, these progressions are comparatively unsuccessful and ineffective. Latest resources and approaches will reduce these limitations. This thesis document is going to proposed a positive and vibrant analysis, concerning on trend analysis which will be effective to decrease and deal with intrusion in ADHOC network. In the ground of intrusion detection, research has been ongoing since about 20 years. Intrusion detection systems appear a second line of defense that recognizes a report attack in real time. Modern world provides the latest system of internet which is disputing for the security of information systems. For the lack of domain familiarity, Intrusion Detection system can fall squat to recognize new attack. To cope with latest attack, database should be rationalized time to time. Possibility of vulnerability to attacks increases for their flexible nature. A few intrusion detection systems which are used for wired network, those are not sufficient for Wireless and ADHOC networks. In ADHOC networks, it is significant for such slant that is proficient to intellect any variety of eccentric actions. In fact, it is out of ability of technology to detect each single contravention. In this research we are going to model an Intrusion Detection System using time series techniques for wireless ADHOC network by which it can detect intrusion. Time series is a technique which can analyze data. Then we will use an unsupervised learning method clustering, to detect intrusion.

Keywords

Intrusion Detection System, IDS, Wireless ADHOC Network, Time Series

1. INTRODUCTION

Security is the major issue for the wireless and Mobile ADHOC network because lack of infrastructure, dynamic network topology, distributed operation, variable capacity links, use of low power devices, limited physical security, and complexity of design of network protocols [1]. Our research project is based on Intrusion Detection. Mounting world cannot imagine even for a single day without computer and computer is basis on internet. Nowadays security of information in internet is becoming very high priority. Modern world emphases in a way by which it can be protect the data and information from any illicit and unauthorized access. Intrusion Detection Systems (IDS) can be differs in various techniques and advance with the objective to detect suspicious traffic in dissimilar ways. There are two significant categories of intrusion detection systems. One is called network-based intrusion detection system (NIDS) and the other one is host-based intrusion system (HIDS). The existing system that detects attacks based on looking for specific signature of identified threats [2]. It reveals particularly that we may have two sets of data; one is of usual and common data and other one apprehensive and suspicious data. So intrusion detection systems match the data with the set of normal and suspicious data and if the deference between the two set is above a threshold value then intrusion is detected [3]. Currently, if Internet infrastructure assault such as man in the middle attack, denial of service attacks and worms infection, have become one of the most serious threats to the network security. It is very likely feasible to detect the attacks and abnormal behaviors if there is sufficient and efficient method and technique exists for monitor and examine, and it can not only make sure proceed warning of potential attacks, but also help out to recognize the reasons, source and locations of the anomalies. By this way, it may assist to restrain the attacks, sooner than they have enough time to broadcast across the network. This document represents the method, in support of detecting Wireless ADHOC network intrusion by analyzing the unexpected change of time series data. With the comparison of other intrusion detection methods, we have focal point on the dynamic behavior of the network using time series analysis and clustering to develop our model [4].

2. SECURITY VULNERABILITIES IN WIRELESS ADHOC NETWORK (MANET)

ADHOC network don't have any central or fixed infrastructure. Every node can move in any direction independently. During the communication of two nodes, the topology of ADHOC network changes rapidly. A great chance of intrusion can occurs during the topology modifies. Because of the dynamic structure security risk is high as well. Marco Carvalho found that MANETs can operate in isolation or in co-ordination with a wired infrastructure, often through a gateway node participating in both networks for traffic relay. MANET's biggest strength are flexibility, self organizing capabilities. On the other hand they are biggest security weakness as well [5]. According to Y Zhang "Intrusion prevention measures such as encryption and authentication, can be used in ADHOC networks to reduce intrusions, but cannot eliminate them. For example, encryption and authentication cannot defend against compromised mobile nodes, which may carry the private keys. Integrity validation using redundant information (from different nodes), also relies on the trustworthiness of other nodes, which could likewise be a weak link for sophisticated attacks" ADHOC network is very sensitive network. Predominantly, Wireless and ADHOC networks are in threat of security attacks. The reason is, ADHOC network comprise the aptitude to modify communications. While we already make out that most of the traffic passes through gateways or routers in wired network. Supplementary security method can be useful at these positions in wired networks. On the other hand, it is beyond feasible in ADHOC network as there is lack of traffic routes. So easily, an attacker can smash up the ADHOC networks by transferring incorrect routing information.

3. RESEARCH BACKGROUND

Intrusion Detection System (IDS) is a software or hardware by which we can detect hackers, malware and bots. There are few types of Intrusion detection system like Network Intrusion Detection System, Protocol-based Intrusion Detection System, Application protocol-based Intrusion Detection System and Host-based Intrusion Detection System etc [7][8].

The consequence of their data analysis point out that Normal system use and behavior trigger low priority alerts for sensor limitation, sensor usages and detection methods limitations Alerts volume can be large and irrelevant alerts require to be removed.

The second step is to create a time series analysis model. The Authors propose three models. These model techniques able to filter out the alerts related to normal flow activities mechanically. All the models use previous observations to predict the current [6].

According to the outcome and assessment of the three models, the accuracy and stability of models are different

Exponentially Weighed Moving Average (EWMA)

- The simplest and the lightest
- Very limited modeling capacity
- -Works surprisingly well in practice for filtering
- With our examples
- Performance can vary with the data set

Stationary autoregressive (AR) model

- Slightly more complex model
- Difficult to interpret and inconsistent
- Limited applicability,
- Non-stationary AR model
- The same AR model
- Continuous estimation
- Accurate
- Consistent and easy to interpret
- Less dependent on data set than EWMA

3.1 Active attacks

Black Hole
Its intentions are not to pass any traffic as all the traffic of the network redirected to a particular node [5].

Sleep Deprivation
A mobile node is forced to exhaust its battery power either by flooding of false messages or by making a mobile node use it battery power on unnecessary processing.

Denial of Service
A mobile node is prevented by attackers either from sending or receiving data packets.

Fabrication of Route Message
Route message with wrong information or malicious contents are injected in the network. Such as false source routing or maximum sequence [5].

Packet Dropping
A mobile node drops data packets on purpose that it supposes to forward.

Spoofing
Inject malicious data or route control packets with modified source address.

Rushing
Protocols have a property that it only accepts the message that it receives first and discard the message that arrives late. Some attackers try to send a malicious control message quickly to block the original and legitimate message that arrives later [8].

3.2 Passive Attacks

Passive Eavesdropping
The attacker may analyze the traffic within the network by pretending himself, without disturbing other traffic.

Selfishness
When a specific node does not serve as a relay to other nodes, some nodes do that on purpose to save their battery power

Motion Pattern Inference Attack
The basic purpose of this attack is to infer the movement patterns of mobile nodes

Location Privacy Attack
The attacker may gather and quantify information about active mobile nodes.

Route Tracing Attack
Route tracing attacks are carried out to monitor the route information against a specific mobile nod[8]e.

4. METHODOLOGY

The environment of the thesis is wireless ADHOC network. ADHOC network does not have any centralization mechanism and it uses the free media "AIR". So it is easy to capture the channel and read the data or steal the important information. Security system of the ADHOC network is poor than any other network. Day by day security vulnerabilities for ADHOC network increases. So for making more secure system of ADHOC network, we use intrusion detection system. By statistical or rule based intrusion detection system, we can detect intrusion and protect information. To make more accurate Intrusion detection system we can use many techniques like time series, regression line, k- means etc. In my thesis

I am using time series to make an intrusion detection model.

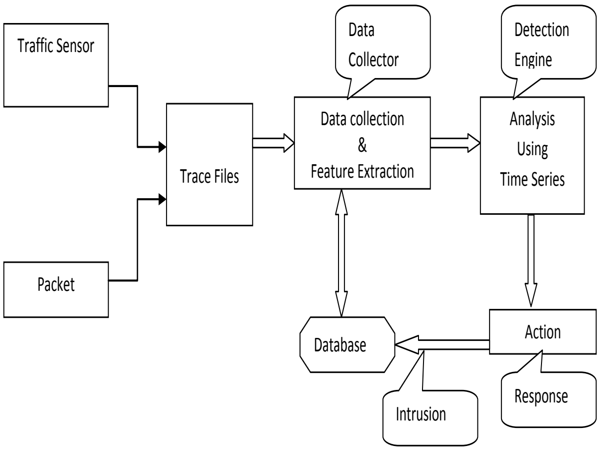


Fig-1: Proposed Model

4.1 Detection scheme

Misuse detection

In misuse detection, The IDS can only detect that intrusion which was already listed in database. The IDS collects the data and match with the database signature like a virus system [11]. Misuse detection IDS try to detect confirmation of unexpected behavior.

Anomaly detection

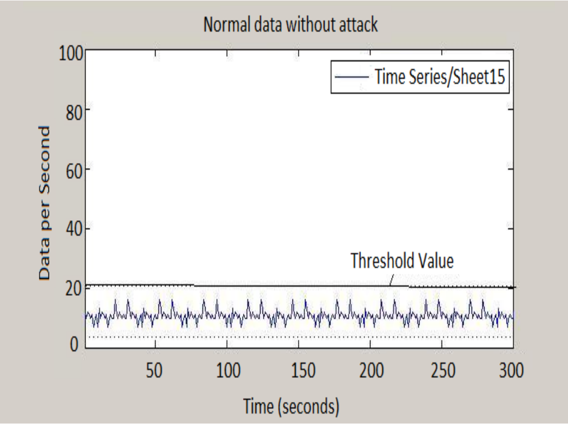
"One disadvantage of anomaly detection for mobile computing is that the normal profile must be periodically updated and the deviations from the normal profile computed. The periodic calculations can impose a heavy load on some resource constrained mobile devices" [12]

Passive system vs. Reactive system

In a passive system, the IDS detect a potential security breach, log the information and signal an alert. In a reactive system, the IDS respond to the suspicious activity by logging off a user or by reprogramming the firewall to block network traffic from the suspected malicious source."

4.2 Traffic analysis and identify attack

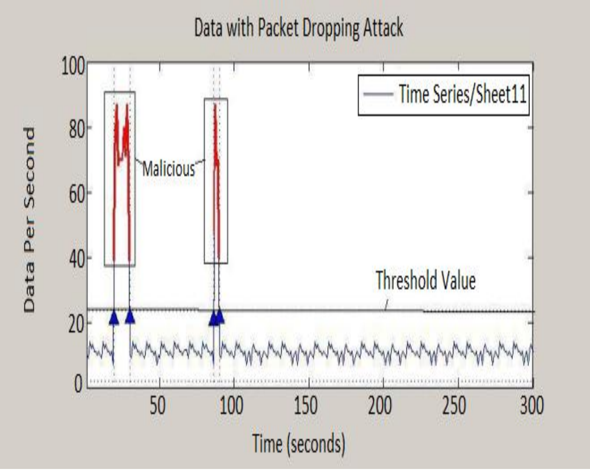
We have described the Network Simulator 2 and its trace file structure. We have also explained the dynamic source routing protocol and the format of the trace file which we used in our data analysis. Then we discussed in brief about time series techniques and how it works in the MATLAB software. The mathematical calculation of Autoregressive model is also discussed in this section. We have gathered all the information from the trace file. In the first field of trace file shows the information about events means packet sends, packet receive or packet drop. Using time series analysis (GUI) tools, we analyze the collected data [17]. We have got dataset without any attack like the following graph.



In this model, we used standard deviation value as threshold value. When data sets hits to the Standard deviation, then alarm will generated for malicious activities. Since standard is not fully depended on previous data so that false alarm rate and misdetection will very low. The accuracy of the intrusion detection rate is approximately 100 percent. One disadvantage of this model is decision delay time. Standard deviation value will be varying with the datasets if there are more data than standard deviation will increase. So it will provide the alarm after confirming that there is abrupt change in data which is intrusion.

False alarm rate = P(D = 0 | H1)

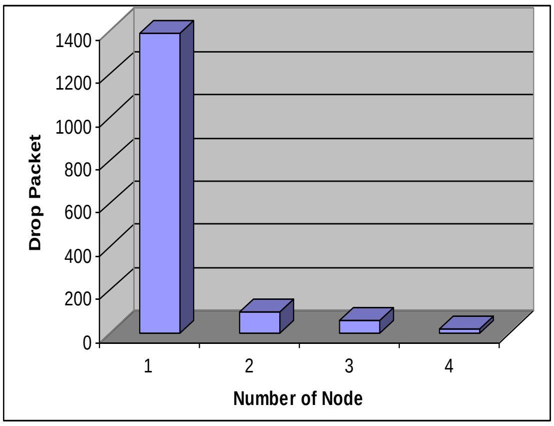
Misdetection = P(D = 1 | H 0)

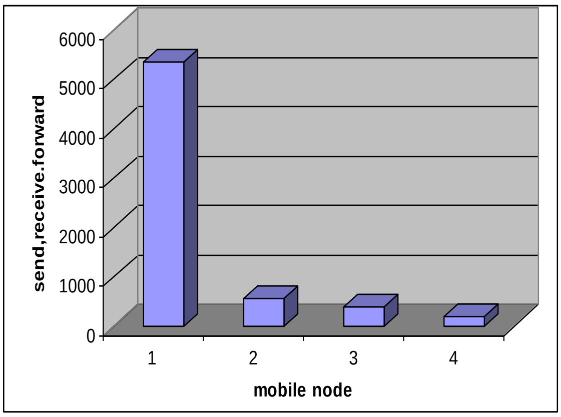


Expected stopping time (aka number of samples, or decision delay time)

5. TESTING AND EVALUATION

The final result of this thesis will show our plan for testing and evaluating our model and results. In this part we also show the calculation of the accuracy and produce some curves to clarify our results.



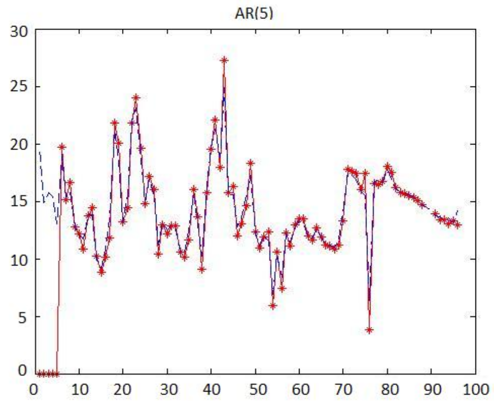


Standard Deviation Model

1. Simple and easy
2. This model does not need to know about the normal data.
3. The confidence intervals automatically reflect this increased knowledge.
4. The confidence intervals based on observed data which is measured to be normal for one user can be significantly different from another [18].
5. It is cost effective than time series model

Time series Model

1. More complex than other model
2. Difficult to interpret
3. More accurate
4. It is quite expensive



6. CONCLUSION AND FUTURE WORK

Though Security is a crucial issue, it plays a vital role in the ADHOC network. Throughout the following discussion of this particular thesis, we have focused on intrusion detection system to identify the network illegitimate activities by using time series analysis. The abnormal changes of network traffic can be detected by analyzing datasets. We have proposed a distributed intrusion detection model which is suitable to detect for vulnerable characteristics of wireless ADHOC network. Our intention was to detect packet dropping attack by identifying malicious and normal behavior through the content of trace file of network traffic.

Our proposed model based on MAC layer of ADHOC network cause almost all the attacks directly influence in the MAC layer. In this proposed intrusion detection model, we have used time series analysis techniques to analyze the data which gathered from the dynamic source routing protocol network trace file. A decision will make when there is a possibility of abnormal activities talking place is very little at a specific time period. It is simple to evaluate trends of behavior throughout the period by time series. But in fact, the main shortcoming of this model is, it is expensive to build compare to other model.

Most of the attack like DoS approaches by packet dropping. If we can detect the packet dropping attack and prevent it then it can protect few other attacks automatically. In our proposed model, we setup a database to store the previous attack for the future use as attack identification.

6.1 Future Work and Limitation

Our project is focused on intrusion detection using time series analysis. During this project we have found few other statistical methods e.g. Mean and Standard Deviation, Logical Regression and so on. In future we want to make intrusion detection model using other methods as well as other routing protocol.

During this thesis,

1. Limited knowledge on MATLAB.
2. It is not possible to do this thesis in practical environment.

7. REFERENCES

[1] Azer M, El-Kassas S, Hassan AW, El-Soudani M. Intrusion Detection for Wormhole Attacks in ADHOC Networks: A Survey and a Proposed Decentralized Scheme. InAvailability, Reliability and Security, 2008. ARES 08. Third International Conference on 2008 Mar 4 (pp. 636-641)

[2] Píštěk M. Zabezpečení podnikové sítě ve společnosti INPOST, spol. s ro, Uherské Hradiště.

[3] Meng L, Dipoala WS, Grimm WM, inventors; Robert Bosch GmbH, assignee. Dual sensing intrusion detection method and system with state-level fusion. United States patent US 7,262,697. 2007

[4] Wu Q, Shao Z. Network anomaly detection using time series analysis. InJoint International Conference on Autonomic and Autonomous Systems and International Conference on Networking and Services-(icas-isns' 05) 2005 Oct 23 (pp. 42-42)

[5] Inam ul haq, 2009, Intrusion detection using K means algorithm in Wireless ADHOC Network, University of Hertfordshire

[6] Amitabh Mishra, KetanNadkarni and Animeshpatcha, Intrusion Detection in Wireless ADHOC networks, February 2004

[7] James Douglas Hamilton, 1994 , Time series analysis, Page 25

[8] Rizwan Qayyum,2006, Security in ADHOC Networks, University of Hertfordshire pp 14-18

[9] YanetManzano, Tracing the Development of Denial of Service Attacks: A Corporate Analogy

[10] Stephen Northcutt ,Network intrusion detection, Third edition, page 271

[11] XuanLongNguyen, 2006, Anomaly and sequential detection with time series data, Y Zhang, Intrusion Detection in Wireless ADHOC Network

[12] Marcov Carvolho(2008), Security in mobile ADHOC network.

[13] Rizwan Qayyum,2006, Security in ADHOC Networks, , University of Hertfordshire pp 14-18

[14] XuanLongNguyen, 2006, Anomaly and sequential detection with time series data, Y Zhang, Intrusion Detection in Wireless ADHOC Network

[15] ÖzleyişOcakoğlu,, A Probabilistic Routing Disruption Attack on DSR and Its Analysis

[16] Anderberg, M. R. 1973 Cluster Analysis for Applications. Academic Press, New York, NY.

[17] John Heideman, 2002 ,IPAM tutorial: Network modeling and traffic analysis with ns-2”, presentation at the UCLA/Institute for Pure and Applied Mathematics, Los Angeles, USA

[18] A Mitrokotsa, 2006, Intrusion Detection of Packet Dropping Attacks inMobile ADHOC Networks