A Methodology for Wireless Intrusion Detection System

Tanvir Habib Sardar
CSE, N.M.A.M. Institute of Technology, Nitte, Karnataka

Zahid Ansari
CSE, P.A. College of Engineering Mangalore, Karnataka

Amjad Khan
ECE, P.A. College of Engineering Mangalore, Karnataka

ABSTRACT
While wireless networks are mounting in reputation and attractiveness, managing these networks for mistreatment and intrusions is not that available. Even though some Intrusion Prevention Systems have come in existence on the market, their effectiveness in intrusion detection are partial. Authentic intrusion detection in wireless networks is not a straightforward add on. This paper discusses a methodology for intrusion detection in wireless network using a cumulative sum algorithm.

General Terms
Computer Networks, Network security, Security Algorithms

Keywords
Intrusion detection system, wireless IDS, cumulative sum algorithm

1. INTRODUCTION
Intrusion detection system is a mechanism to sense intrusion of adversaries to act in response and reduce the harm. Intrusion detection system in WSN‟s protocols is planned without safety in intellect so they require an intrusion detection system that monitors packets on the network and effort to find out if a hacker/cracker is trying to rupture into a system.

An Intrusion detection system (IDS) is software and/or hardware deliberate to detect surplus attempts at accessing, manipulating, and/or disabling of computer largely throughout a network, such as the Internet. An intrusion detection system is created to become aware of quite a few types of malicious behaviours that can negotiate the safety and faith of a computer system. This includes network attacks alongside susceptible services, data driven attacks on applications.

An Intrusion Detection System (IDS) is a arrangement that is in charge for detecting irregular, inappropriate, or other data that may be measured illegal happening on a network. An IDS captures and inspects all traffic, in spite of of whether it's legalized or not. Based on the contents, at either the IP or application level, an alert is made.

According to the NIST‟s records on industry best practices, these are a number of convincing reasons to obtain and make use of IDS:

1. To put off trouble behaviours by growing the apparent danger of discovery and publish for those who would attack or otherwise mistreatment the system.
2. To become aware of attacks and other safety violations that is not prevented by other security measures.
3. To perceive and deal by means of the preambles to attacks (commonly skilled as network probes and other “”doorknob rattling‟ activities).
4. To document the existing threat to an institute.
5. To take action as quality control for security control for security design and administration, particularly of large and complex enterprises.
6. To offer helpful information concerning intrusions that do happen, allowing improved diagnosis, recovery, and correction of contributory factors.

Intrusion detection strategy is an integral part of any network. The internet is constantly developing, and new vulnerabilities and exploits are found frequently. They make available an extra level of guard to sense the presence of an intruder, and assist to provide responsibility for the attacker's action.

An ***Anomaly-Based Intrusion Detection System*** is a system for detecting computer intrusions and exploitation by monitoring system motion and classifying it as either normal or irregular. The categorization is based on heuristics or rules, rather than patterns or signatures, and will detect any type of exploitation that falls out of normal system process. The most widespread way people move towards network intrusion detection is to notice statistical anomalies.

The thought at the back this approach is to compute a "baseline" of such states as CPU consumption, disk activity, and user logins, file activity, and so forth. Then, the system can set off when there is a divergence from this baseline. The advantage of this move towards is that it can detect the anomalies without having to recognize the fundamental cause behind the anomalies. So as to decide what attack traffic is, the system must be taught to be familiar with normal system activity. This can be accomplished in numerous ways, most often with artificial intelligence type techniques. Systems using neural networks have been used to huge outcome. Another means is to describe what regular usage of the system comprises using a strict mathematical representation, and flag any deviation from this as an attack. This is identified as strict anomaly detection.

A ***network intrusion detection system*** is a technological tool that checks on a variety of performance on your network. For instance, you can supervise the in-and-out flow of data and monitor network traffic by installing NIDSs in your network. There are specific points in the network where NIDSs are installed to make sure the traffic to and from all the other computers installed in the network.

Based on a signature, rules or any suspicious patterns, every single incoming packet is checked and detected by NIDs. Presume you examine abundant TCP link sending requests to a lot of dissimilar ports. Subsequently you can wait for that an unauthorized user is trying to carry out a port scan on a small number of or the entire computer in your network. Besides incoming network traffic, NIDS can perceive any intrusions going on from outgoing traffic additionally. If an attack has been launched from inside of your network section, it will not be engaged as incoming traffic. Network intrusion detection systems typically associate with other systems and security tools. This means that they are able of updating blacklist of some firewalls with the IP addresses that were used by attackers. A NIDS does not obstruct the network traffic at all, nothing like a firewall or packet filter. Just put, NIDSs take action as packet sniffers and carry out an study of the captured packets[1].

A ***signature-based IDS*** checks traffic looking for patterns that match known signatures that is, preconfigured, prearranged attack patterns. Signature-based IDS technology is extensively used because a lot of attacks have clear and dissimilar signatures, for example: (1)foot printing and fingerprinting actions, contain an attack pattern that includes the use of ICMP,DNS querying ,and e-mail routing investigation;(2)exploits occupy a exact attack series designed to obtain benefit of a susceptibility to gain access to a system; (3) denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks, throughout which the attacker put effort to put off the normal practice of a system, involve overloading the system with requests so that the system's capability to process them efficiently is compromised/disrupted and it begins denying services to official users.

An additional flaw of the signature-based process is the time frame over which attacks take place. If attackers are decisively slow and methodical, they may slip unnoticed through this type of IDS because their performance will not equivalent those of their signatures, which frequently comprise the occasion allowed amid steps in the attack. The only method for signature-based IDS to determine this susceptibility is for it to gather and analyze data over longer periods of time, a procedure that takes considerably big data storage space capability and other processing capacity.

Wireless Sensor Network (WSN) consists of spatially spread autonomous sensors to jointly monitor physical or environmental circumstances, such as temperature, sound, vibration, pressure, motion or pollutants. It consists of thousands of sensor nodes have a lot of possible applications nowadays from temperature, light monitoring in a smart house to detecting enemy's association in a battle field.

As a general rule, sensor networks are deployed in open and defenceless environments so it is extremely striking to adversaries. There are a lot of habits adversaries be able to use to attack sensor networks [2][3]. Even though some preventive mechanisms were projected and installed, they do not promise the security of sensor networks one hundred percent. So, it is essential to encompass some mechanisms of intrusion detection as a instant protecting wall to prevent intruders from causing damages to the networks.

As well to one or more sensors, each node in a sensor network is characteristically equipped with a radio transceiver or other wireless communications device, a little microcontroller, and an energy source, frequently a battery[4]. A sensor node might differ in mass from that of a shoebox down to the size of a grain of dust, though functioning "motes" of authentic microscopic dimensions have yet to be shaped. The price of sensor nodes is likewise changeable, ranging from hundreds of dollars to a small number of pennies, depending on the complication of the individual sensor nodes. Size and cost constraints on sensor nodes result in matching constraints on resources such as energy, memory, computational speed and communications bandwidth.

A sensor network usually constitutes a wireless ad-hoc network, meaning that each sensor chains a multi- hop routing algorithm where nodes function as forwarders, relaying data packets to one of more "base stations". The progress of wireless sensor networks was originally enthused by military applications such as battlefield surveillance. Though, wireless sensor networks are now used in a lot of civilian application areas, including surroundings and habitat monitoring, healthcare applications, host size and cost constraints on sensor nodes result in matching constraints on resources such as energy, memory, computational speed and bandwidth.

A sensor network usually constitutes a wireless ad-hoc network, meaning that each sensor supports a multi-hop routing algorithm, automation, and traffic control.

2. EXISTING WORK

Intrusion Detection is not a new research issue in the broad area of security. A lot of work has been done so far for Intrusion Detection in wired conventional networks [5], [6], [7], and [8]. However, limits of WSNs make the direct calculated. A larger than common time will point towards a wormhole attack. This approach requires firmly the clock synchronization among nodes in the network which is not easy to gain in WSNs.

In [10], the author proposed two statistical approaches to detect wormhole attack in WSNS. The first one called Neighbour Number Test bases on a simple statement that a wormhole will increase the number of neighbours of the nodes in its radius. The base station will get neighbourhood information from all sensor nodes, computes the hypothetical distribution of the number of neighbours and uses statistical test to make a decision if there is a wormhole or not. The second one called All Distance Test detects wormhole by computing the allocation of the length of the shortest paths amidst all pairs of nodes. In these two algorithms, most of the workload is done in the base station to save sensor nodes resources. However, one of the chief shortcomings is that they do not identify the location of the wormhole which is necessary for a proper defence.

A rule-based algorithm was proposed in [11] to detect anomalies in WSNS. Monitor nodes will make sure traffic on their neighbours and compare to some predefined rules. If a rule is not contented, a failure is accumulated. An anomaly is reported if the number of crash is greater than an expected value which is calculated dynamically by the monitor node. However, some rules are not easy to put into practice and resource consuming. More important, the detection efficiency and accuracy depend on the buffer size which is strictly limited in WSNS. A similar algorithm proposed in [12] has the same drawbacks.

3. PROPOSED WORK

A lot of techniques have been done for anomaly detection such as: neural network, audit data analysis and application of these solutions unsuitable. Intrusion detection in WSNs is getting more and more notice of researchers. However, there are a restricted number of papers about algorithms to detect attacks in WSNs so far. One of them is the "temporal packet leashes" algorithm used to detect wormhole attack [9]. In this approach, the time essential to transport a packet among each pair of neighbours will be mining, statistical models. Each of them has their own pros and cons. Here, we used a widely-used anomaly detection algorithm, Cumulative Sum (CUSUM). CUSUM is suitable to deploy in sensor network because it is a strong, light-weight and less memory consuming statistical model.

CUSUM is one of some change point detection algorithms used widely to detect the change of the mean value of a random sequence [13], [14]. In brief, CUSUM detect changes based on the cumulative effect of the changes made in the random sequence instead of using a single threshold to check every variable.

4. METHODOLOGY

Because of the be deficient in of middle point to gather data, our Intrusion Detection System is distributed. That means some nodes, called monitor nodes, will be installed Intrusion Detection Agents to protect themselves and their neighbours (called monitored nodes). Monitor nodes are selected so that every node in the network is monitored by at slightest one monitor node. One node can be monitored by quite a few monitor nodes. There is a trade-off connecting security level and resources. The more monitor nodes, the highest security level.

Fig.1 shows the architecture of a monitor node. This node runs the common node functions, like sensoring and data message sending and retransmitting, besides the IDS functions. IDS functions are completed in the immoral listening node in which the node captures all coming packets, analyzing and detecting irregular behaviours. This architecture is similar to the architecture proposed by R. Da Silva in [2]. The major different point here is the "Anomaly Detection" module.

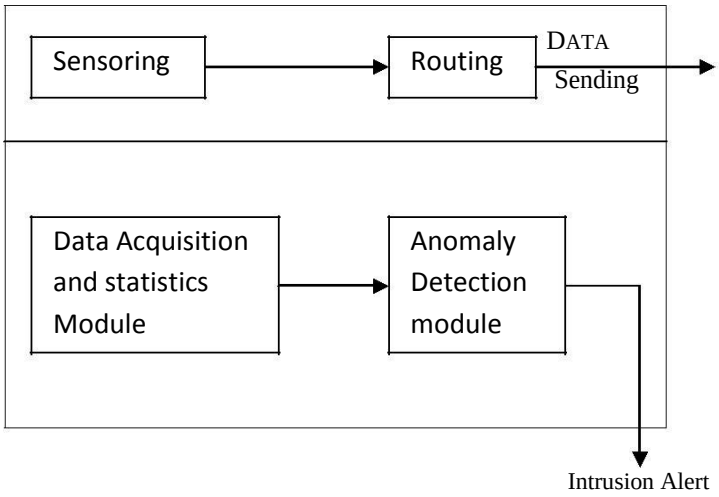

Fig. 1 Architecture of a node

Data will be used by the anomaly detection module to detect abrupt changes. The data acquisition module and anomaly detection module details are clearly described in the coming sections. The structure chart diagram for intrusion detection is shown in figure 2.The calling sequence is from top to down and left to right. The execution of the mechanism follows these steps:

On execution the server running frame is opened, which needs to be run indicating now the server is waiting for a request from a client.

Running causes the multithread chat server class usage in server package. The method start server indicates the server is associated with a socket and when a request comes from a client a socket is created for the client. A separate thread starts running for the newly connected client.

This package makes use of client package which implements data acquisition and statistics module.

This module calculates the number of incoming and outgoing packets from connecting node.

The client is configured in client frame.

The details of the client and incoming and outgoing packet count are passed to the server package for implementing anomaly detection module.

The CuSum algorithm is implemented in this module. This module calculates the change in the incoming packet count and on dividing this with average number of packets a test value is obtained.

This module checks this test, value with a threshold. If the test value exceeds threshold intrusion details are displayed in a server frame otherwise intrusion not detected will be reported. Finally the intrusion details can be analyzed by using intrusion model and intrusion service classes. These classes will access the database contents.

The threshold model and threshold model and threshold service class are used to set threshold value. This data will be inserted into the database using these classes and later it is retrieved from the table by multithread chat server class for algorithm execution.

Since a WSN is simulated in our project we have restricted the number of nodes to 10. In order to establish a communication between the sender and destination node, first the sender node need to send a connection request to destination node .The destination node listens for all requests via a port The client talks to the server by writing to the socket and gets information from the server by reading from it. Similarly, the server gets a new-local port number. The server also binds a socket to its local port and communicates with the client by reading from and writing to it.

Once a request is accepted, the destination node creates a socket to communicate with the sender node. Once connection is established the sender node can send a request to destination node. All the requests will be translated as packets and the incoming and outgoing packet count is noted. The two modules data acquisition and anomaly detection module make use of this count. The data acquisition module captures the packets and counts the incoming and outgoing packets.

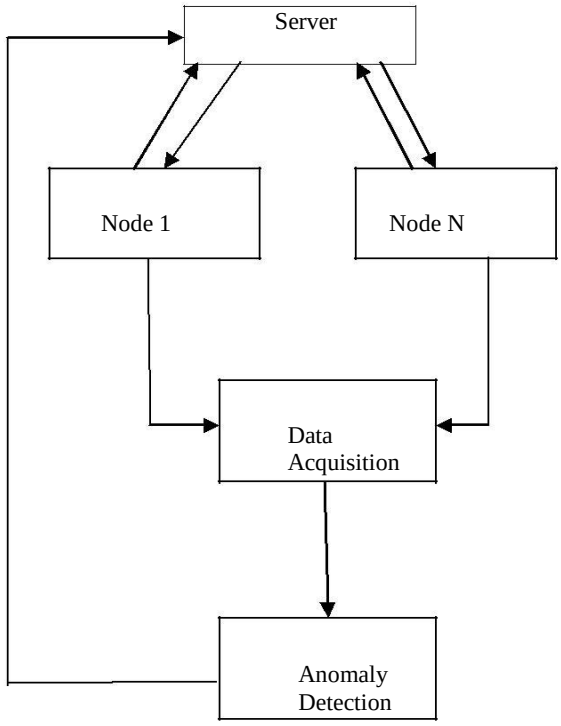

Fig. 2. Structure chart diagram of intrusion detection

5. CONCLUSIONS

The aim of the work is to simulate a Wireless Sensor Network to show how system detects an intrusion using Cumulative Sum algorithm which is considered light-weight and powerful to detect abrupt changes in a random sequence. Suppose that the network has k nodes, the Cumulative Sum algorithm shows us that the complexity in each step (each sampling period) is O (k). In common sensor networks, k is often less than 10 so the node just needs to do some basic operations in each sampling period. By comparison, the rule based algorithms [12],[15] have to analyze and check traffic data with a series of rules some of which are not straightforward and require a considerable amount of computational resource.

Besides, little amount of memory resource is required by our algorithm. The node just allocates memory for some trivial variables and a small-size array for statistics data of packers of the neighbours. In rule based algorithm they need a huge buffer to store all packets needing to be analyzed and the algorithm turns out poor result with a small-size buffer [13],[14].

However, simulation is needed to prove strongly the result of this algorithm. In addition, nodes in our system should work in cooperation to detect intrusion faster and with higher accuracy. These drawbacks are what mainly focused on to improve the intrusion detection system.

The present system only detects SYN-flood attack. This can be extended to detect other attacks also. The present system is shown through the simulation, and this can be implemented in real sensor network. We have done intrusion detection. In many organizations intrusion detection is not just sufficient. There are many cases intrusion can result in lot of service problems. Thus intrusion prevention systems should be there to prevent subsequent failures due to intrusion. Now a day's intrusion detection and prevention system (IDPS) plays an important role .Whenever an intrusion occurs to a network a simple IDS will just warn the administrator to do any preventing actions. The administrator either have to reconfigure firewall or should have some mechanism to block the traffic that deviates from normal behaviour .Thus future work have to be done with these in mind having an intrusion prevention systems along with detection.

6. REFERENCES

[1] I.F. Akyildiz, W.Su,Y. Sankarasubramaniam and E.Cayirci:Wireless sensor networks: A survey, Computer Networks, 38(4):393--422, March 2002.

[2] Anthony D.Wood and John A.Stankovic: Denial of service in sensor networks,IEEE computer,October 2002,pp 61-62.

[3] C. Karlof and D. Wagner: Secure Routing in Wireless sensor networks:Attacks and Countermeasures, Ad Hoc Networks, vol. 1, pp. 293-315, 2003 .

[4] Yi-an Huang , Wei Fan , Wenke Lee , Philip S. Yu: Cross feature analysis for -Detecting Ad-Hoc Routing Anomalies, Proceedings of the 23rd International Conference on Distributed Computing Systems, p.478, May 19-22, 2003.

[5] K. Ilgun, R. A. Kemmerer, and P.Porras State transition analysis A Rule Based intrusion detection approach, IEEE Trans on Software Engineering, 21 (1995), pp. 181–199.

[6] Jake Ryan,Meng-Jang Lin,Risto Intrusion detection with Neural Networks, Advances in Neural Information Processing Systems 10 (Proceedings of NIPS'97, Denver, CO), MIT Press, 1998.

[7] P. A. Porras and P. G. Neumann: Emerald: Event monitoring anomalous live disturbances, in Proc of 20th NIST-NCSC Nat‟l Info Systems Security Conf, 1997, pp. 353–365.

[8] M.-Y. Huang, R. J. Jasper, A large scale distributed intrusion detection framework based on attack strategy analysis, Computer Networks, 31 (1999), pp. 2465–2475.

[9] Y. Hu, A. Perrig, and D. Johnson: Packet leashes a defense against wormhole attack in wireless ad hoc networks. In Proceedings of the IEEE Conference on Computer Communications (Infocom), 2003.

[10] Levente Buttyán, László Dóra, István Vajda: Statistical Wormhole Detection in sensor networks:ESAS 2005:128-141.

[11] V. A. Siris, F. Ppapagalou: Application of Anomaly Detection Algorithms for Detecting SYN Flooding Attacks, Global Telecommunications IEEE 2004.

[12] Haining Wang, Danlu Zhang, and Kang G Detecting SYN-Flooding Attacks, IEEE INFOCOM'2002, New York City, NY, 2002.

[13] M. Basseville and I. V Nikiforov Detection of abrupt changes Theory and Application, Prentice Hall, 1993.

[14] B.E. Brodsky and B.S. Darkhovsky A non parametric methods in change point Problems, Kluwer Academic Publishers, 1993.

[15] Riaz A. Shaikh, S.M.H. Zaidi, Saeed Rajput and Kashif Shar Review over anomaly detection algorithms for detecting SYN-Flooding attacks 4th Annual IEEE Student Conference on Engineering Sciences and Technology (SCONEST 2005), Karachi, Pakistan.