ISSN: 2320-8090

Available online at http://www.journalijcst.com

International Journal of Current Science and Technology
Vol.5, Issue, 4, pp. 385-389, April, 2017

IJCST

RESEARCH ARTICLE

SECURITY IN AD HOC WIRELESS NETWORKS

Douglas Omwenga Nyabuga., Zhao Chen*., Guohua Liu and Ting Lu

Research Scholar in Computer Science and Technology Donghua University, Shanghai (China)

ARTICLE INFO

Article History:
Received 15th January, 2017
Received in revised form 8th February, 2017
Accepted 24th March, 2017
Published online 28th April, 2017

Key words:
Ad Hoc wireless networks; Intrusion Detection Systems; Node

ABSTRACT

Ad Hoc wireless networks is a wireless type of network connection which is established without a central device as a router but on a flexible and dynamic infrastructure. Usually the users are very comfortable in using a secure system. Due to flexibility and dynamic features of this network it's therefore vulnerable to various attacks; the signal strength is too weak and it isnot easy to monitor the transmission of data from the source to the destination and vice versa. This study is aimed at looking various methods that have been used to address the issues with security threats in big data collected from the network, the design vulnerability of ad hoc wireless networks and propose the best real time metrics and algorithms for data encryption to prevent attackers from accessing the data on transmission; strong communication rules a need to control and check the unwanted or unauthorized access to the backhaul of the network and thus protect the network from IP spoofing and denial of services.

INTRODUCTION

An ad hoc wireless network is a wireless type of network that enables computers to connect and communicate without a central connection device such as the router to share resources such as data or files [1].An ad hoc network requires that the computers or devices be within proximity as the wireless network is limited with distance and physical obstacles. Therefore, if the computers or devices connected to an ad hoc wireless network goes out of sight, the other devices are disconnected automatically. To better understand how to identify and protect the information systems and networks from cyber-bouts in ad hoc wireless networks, requires an understanding of what an ad hoc wireless network is. The proliferation of the Internet access and usage has resulted in the drastic growth of network vulnerabilities. Network vulnerability causes cyber-bouts through which the attackers break into the system that is connected to the network. For example, attackers employ various types of Denial of Service (DoS) attacks as a type of cyber-bouts on the network that can immediately cause system failure. Therefore, this study is to identify network cyber-bouts before they can damage network system and to address the challenges faced by ad hoc wireless networks in the real-time. Since an ad hoc wireless network allows any node within the network to connect, these poses a huge risk of exposure to attacks thus the security of the systems or devices becomes a big challenge. The ad hoc wireless network supports a small amount of bandwidth; therefore as the number of systems increase, the strength of the signal becomes weaker thus performance is adversely affected by the number of systems on the network.

Corresponding author: Zhao Chen
Research Scholar in Computer Science and Technology Donghua University, Shanghai (China)

The monitoring systems deployed must have the capability to detect the suspicious activities of a large amount of data received from the networks and filter it out to capture the threats that might be carried with it. Coming up with the real-time monitoring and detecting systems is tough because handling a large size of data on the network is not easy and the ad hoc wireless networks are difficult to monitor especially when the ad hoc wireless network changes the site or location is detrimental in managing an ad hoc network [2], [3], [4], [5]. These have resulted in the proliferation of various kinds of attacks that are difficult to manage especially those that target business networks and other information systems.

The methodologies used in ad hoc wireless networks

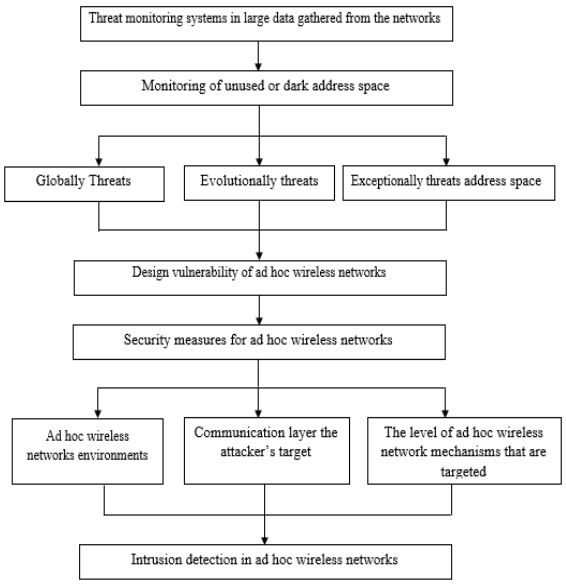

Figure 1 The methodologies used in ad hoc wireless networks

Threat monitoring systems in large data gathered from the networks

As the number of sources and the volumes of data increases, big data challenges also increases particularly in the monitoring system that filters volumes of data from its sources. Big data technologies can try to help to solve these problems through incursion discovery. Through the use of intrusion detection systems for monitoring enables the discovery of misuse or anomaly detection that can be used by potential attackers in the big data and many sources. This technology can be employed in the discovery and monitoring of the misuse and any anomaly in the database with matching of attack signatures to determine their matches. Also, Network Intrusion Detection System (NIDS) can be used to monitor the threat detection in big volumes of data in the network by filtering the network traffic. Moreover, the host-based intrusion detection systems monitor the host computer logs, files and network interface as well [6].

The big data at the moment is encountering a significant challenge due to the increase of false alarms and ambiguous flow of data. For example, a big company or organisation can have all the latest technologies like firewalls, the intrusion detection systems, the powerful antivirus software and other security systems but monitoring the threats is a difficult task to accomplish [7]. To improve the intrusion and anomaly discovery, all the monitoring systems involved must be correlated with each other to increase warning accurateness instead of the false alarms [8]. Additionally, large enterprises or organisations are facing challenges of handling, storing and processing big volumes of data. This forces the companies to have different formats of data storage like a relational database which leads to a huge problem to correlate the events of that large amount of data because data might be stored at different locations and servers. How to manage the various sources of data through the network are significantly a challenge and the security issues it comes with it [9]. In the past security, monitoring was mainly handled by the system administrator checking the log files of their servers. This has changed as it is not easy to monitor the big amount of data on the network, and the collection of it and even the systems that are used in the monitoring cannot cope well with the big data challenge.

Data fusion technique should be adopted as an intrusion detection strategy. Data fusion technique has the capability of aggregating data from various kinds of sources such as system log files, system messages, SNMP traps and queries, many distributed packet sniffers, and operator commands. Also, the Distributed Intrusion Detection System (DIDS) model can be used as an intrusion detection strategy. Therefore, data fusion technique and Distributed Intrusion Detection System (DIDS) model seek to increase overall accuracy and detect more threats. It can also accommodate various sources, and their study gives examples of different event sources. Distributed Intrusion Detection System (DIDS) has distributed IDS nodes that are referred to as “sensors”, which have the capability to conduct data fusion to correlate different event types (if they are in different formats). Overall, every "sensor" IDS can communicate with every other sensor in the network with the motivation of redundancy as well as extra-resiliency against attacks.

To address the problem posed by large volumes of data from various sources within the network the researcher proposes the use of Hadoop and a network monitoring tool known as PacketPig for quality protection of data. The big companies or organisations can also deploy tools like a beehive for log file analysis to discover suspicious activities and questionable destinations in the organization’s networks [10].

Monitoring of unused or dark address space

Because there are no legitimate hosts in an unused address block, traffic must be the result of misconfiguration, backscatter from spoofed source addresses, scanning from worms and probing. These pre-filtering provides an excellent technique of studying and monitoring Internet threats.

Ad hoc wireless networks connection leaves network assets vulnerable to the rapidly moving threats of today’s Internet, including fast moving worms, distributed denial of service attacks, and routing exploits. These threats share several key properties. First and foremost these threats are globally scoped, respecting no geographic or topological boundaries. In some cases they are zero-day threats, exploiting vulnerabilities for which no signature or patch has been developed, making detection and mitigation of these threats a big task. Second, these threats are evolutionary, with each worm or attack learning from previous failures, spawning an arms race between the network defenders and the attackers. Finally, many of these threats are exceptionally infectious, transmitting to the entire vulnerable population in the Internet in a matter of minutes, making the human response impractical.

Monitoring of unused or dark address space is investigating technique used with a snapshot of global Internet worm activity. Another method to increase visibility of the internet threat is to monitor larger blocks of address space. The challenge with is that the IPv4 space is limited and there are a small number of large unused address blocks available for consideration. Address blocks in different networks see different threat traffic [11].

An algorithm for checking the dark address spaces

```
#include "d_crypt.h"
void main()
{
   int ie;
   string_o sins("This text will be encrypted with Rijndael\n");
   string_o sout, sret;
   string_o skey1("the password has 32 characters.");
   string_o skey2("checking the position words");
   multicrypt_o x;
   x.set_uucoding (multicrypt_o::UU_YES_STRIPPED);
   x.add_crypto ("aes", skey1, "", &ie);
   x.add_crypto ("des", skey2, "", &ie);
   x.encrypt (sins, sout, &ie);       // sout: encrypted string
   x.decrypt (sout, sret, &ie);       // sret: decrypted str (==sins)
}
```

Design vulnerability of ad hoc wireless networks

Ad Hoc wireless networks being a wireless type of network is more vulnerable to attacks compared to the wired type of network. Some active attacks like denial of service are common to the ad hoc wireless network due to the flexibility and dynamic change of ad hoc wireless network [9].

Because of the dynamic design and flexibility features of the ad hoc wireless network, it makes it weaker and vulnerable to attacks through the nodes that build up the network system. Since an ad hoc wireless network is a wireless type of network, its lack of a central device such as the router makes it very difficult to manage the nodes within the network thus there is a lack of the authentication.

Due to lack of centralised device, the nodes within the network acts as the router are not trustworthy as a result of that they pose a serious security within the network. With the flexibility and dynamic of the ad hoc wireless network, there might be malicious nodes that can quickly join the network which makes it prone to malicious node attacks and false routing.
The security measures in ad hoc wireless network such as the confidentiality, authentication, non-repudiation, integrity are tough to be realized due to lack of a static network.

It can be looked at as a directed graph where each node wants to communicate with each other within the network

$\boldsymbol{G\ (V, E)}$,Where each node **V** is comprised of the set of vertices nodes together with a set $\boldsymbol{E}$of edges or lines, which is a subset of $\boldsymbol{V\ X\ V}$

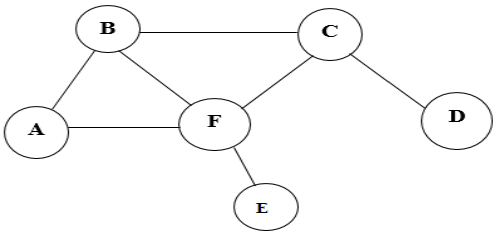

Figure 2 Interconnected nodes on Ad Hoc wireless network

$$G = (V, E), V = \{A, B, C, D, E, F\} \quad (1)$$

$\boldsymbol{E}$ =
$\{(A, B), (B, A), (A, F), (F, A), (B, F), (F, B), (E, F), (F, E), (B, C), (C, B), (C, E), (E, C)\}$ (2)

There is possible traffic of packets from different nodes within the network; the attacker can focus on disrupting the routes on the network through its neighbour with bogus information that is an authorised participant that might be malicious which leads to denial of services to the other neighbour nodes in the network. It is tough and challenging to address the vulnerabilities within the ad hoc wireless networks due to dynamic of the network [12], [13], [14]. There are some possible attacks such as denial of services which might occur as a result of the failure of a node(s), and jamming that tampers with spectrum in the nodes [4], [15], and [16]. The internet protocol collisions attack is caused when two nodes try to transmit information on the same spectrum which leads to rejection of transmission of data packets. Other attacks include flooding attack in which the attacker makes several connection requests until a maximum limit is reached and thus causes unavailability of the resources in the network and data integrity which the attacker uses to alter the data on transmission among the nodes which leads to disruption of operations. To handle this, digital signatures and the asymmetric key system can be deployed to prevent such attacks.

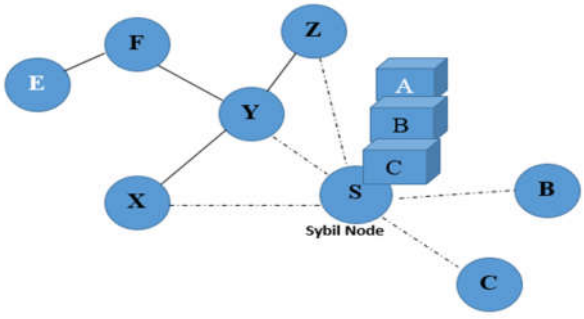

Figure 3 The Sybil attack

The Sybil attack above it tries to damage data integrity and utilisation of resources within the ad hoc wireless networks; this can be addressed by the use of encryption and authentication algorithms to prevent the attacker from the attacks. A sample of encryption and decryption algorithm that can be used in the defending of authenticity, integrity and confidentiality of services:

String passcode = Bitshifter.*encrypt*(plainText);
System.***out***.println("Encrypted Text After Encryption: " + passcode);
System.***out***.println("Decrypted Text After Decryption:" + Bitshifter.*decrypt*(passcode));
This makes it harder for the attacker to break through the encrypted message or data as is transmitted on ad hoc wireless networks

Security measures for ad hoc wireless networks

Internet users are continually encouraged to use a secured network. So, it is important to provide ad how wireless network with trustworthy security mechanisms if we want to see this exciting technology become broadly used in the future. Before the development of any security measure to secure ad hoc networks, it is important to study the variety of attacks that might be related to such networks. With the knowledge of some common attack issues such as how ad hoc wireless networks could be threatened by the attackers, and thus might lead to the development of more reliable security measures in protecting them.

Ad hoc networks environments

Ad hoc wireless network can exist in one of three environments; organized, localized, and open environments. Nodes in all of these environments are generally threatened by the same security problems. However, there are some security problems, that are unique to one environment and need more attention in that environment than the others need. Vast numbers of unstructured nodes and the absence of a priori relations are some of the main characteristics of the open environment ad hoc wireless networks. Such networks are quite similar to the localized environment networks, but the larger amount of nodes, and the wider coverage area, renders nodes in the open environment to more sophisticated security attacks than the localized networks do. For instance, nodes in both open and localized environments suffer from the absence of a central authority.

Communication layer the attacker's target

Each layer in the ad hoc wireless networks communication protocols is vulnerable. In a physical layer, ad hoc wireless network nodes as well as the communication links are vulnerable to both passive and active attacks. Passive eavesdropping, signal jamming, denial of service (DoS) attacks, and physical hardware tampering are among the most popular attacks in this layer [17]. Such attacks prevented by encrypting the communication link, employing spread-spectrum communication technology, and using a tamper-resistant hardware.

The level of ad hoc network mechanisms that are targeted

There are two main levels of attack in the ad hoc wireless network; attacks against the basic measures and attacks against the security mechanisms [18]. Ad hoc networks have their own

unique basic mechanisms, such as the use of wireless links for communications, employing their own routing strategies, and operate in a distributed manner all these basic mechanisms actually reflect their own unique characteristics that differentiate them from other types of networks. Attackers might launch many security attacks against these basic mechanisms. For instance, attackers could launch passive eavesdropping attacks against the wireless links, drain off node's limited resources, and launch active attacks to interrupt the routing mechanisms.

To address many security attacks against the ad hoc network basic mechanisms, a number of security measures have been introduced to protect the networks. Still, all these security measures are also vulnerable to attacks and need to be secure. Stealing username and password to get unauthorized access in the networks and modifying public key databases to disrupt authentication, confidentiality, and integrity services are some examples of attacks against security mechanisms.

Intrusion detection in ad hoc wireless networks

In order to mitigate or prevent attacks, awareness of an attack is essential to being able to react and defend against attackers. Prevention can be further improved by utilizing security analytics and intrusion detection data to look for hidden attack patterns. Intrusion detection s very helpful in detecting cyber-attacks in noticing abnormal system behavior to detect accidents or undesired conditions and provide early warnings to mitigate damages.

For Intrusion Detection, large amount of data is currently a major challenge and has been a prevailing theme for quite some time. According to Frank (1994) [19], Intrusion Detection focusing on data reduction and classification found: "a user typically generates between 3-35 Megabytes of data in an eight hour period and it can take several hours to analyze a single hour's worth of data". Data filtering, clustering, and feature selection is "important if real-time detection is desired," which can improve detection accuracy that the huge data is facing.

While a more comprehensive security monitoring system across diverse systems could improve security, it would further worsen the large data challenge for intrusion detection which is already present in isolated systems. Integrating across more security sensors would increase large data issues in terms of: Volume in having to store more information collectively, Velocity in that more information would be flowing collectively at a higher rate in and out of the monitoring system, and especially Variety in terms of many different types of information coming from very different sources and also collectively yielding higher dimensionality.

A more comprehensive approach for monitoring a numerous of diverse event sources for intrusion detection can yield a better situational awareness of the threats in ad hoc wireless networks, and thus improve detection accuracy and minimize false alarms by correlating security events among these diverse sources. When large data challenges are already present in any of the underlying inputs or outputs for intrusion detection, the overall system will likely experience large data challenges as well unless the large data challenge is eradicated. One way to eradicate this large challenge is by filtering out (removing) the large data from a subsystem. However this is not ideal if valuable information is lost. New techniques can alleviate the challenges and costs that large impose for intrusion detection.

Step 1: Large data formation

One input is deemed Large Data and is added to another input which is not Large Data, the result will still be Large Data. This can be shown in Equation 1 below:

LD(LargeData") + NLD ($NotLargeData$) = LD ($LargeData$") (3)

Step 2: In Equation 2 below (where the subtraction operator is essentially filtering or removal of the Large Data):

$$LD\ (\text{"LargeData"})\text{-LD ("LargeData"}) = NLD\ (\text{"NotLargeData"}) \quad (4)$$

Proposed solution to the hurdles of ad hoc wireless networks

This paper, therefore, proposes that communication channels must be secured using sophisticated algorithms for data encryption to prevent attackers from accessing the data on transmission. Also, there is a need to control and check the unwanted or unauthorised access to the backhaul of the network by the development of strong communication rules which will protect the network from IP spoofing and denial of services. Moreover, there is a need of using filter software to detect malicious and suspicious threats and block them from accessing the systems and synchronise network security with the network traffic management to increase the security of Ad-hoc wireless networks.

Acknowledgment

This work was supported in part by the Young Scientists' Sailing Project of Science and Technology Commission of Shanghai Municipal under Grant 17YF1427400 and in part by the Fundamental Research Funds for the Central Universities under Grant 17D111206.

References

1. Pinola, M. (2016, September 12). lifewire. Retrieved from lifewire: www.lifewire.com
2. G. Xu, W. Yu, Z. Chen, H. Zhang, P. Moulema, X. Fu and C. Lu. (2015). A cloud computing based system for cyber security management. *International Journal of Parallel, Emergent and Distributed Systems*, 30(1): 29-45.
3. V. Yegneswaran, P. Barford, and S. Jha. (2004). Global intrusion detection in the domino overlay system. In Proceedings of the 11th IEEE Network and Distributed System Security Symposium (NDSS).
4. W. Yu, N. Xu, Z. Chen, and P. Moulema. (2013). A cloud computing based architecture for cyber security situation awareness. In Proceedings of 4th International Workshop on security and Privacy in Cloud Computing (SPCC).
5. W. Yu, N. Zhang, X. Fu, R. Bettati, and W. Zhao. (December 2010). Location leakage of internet threat monitors: Modeling and defense. IEEE Transaction on Computers (TC), (pp. 59 (12): 1655-1668).
6. Nassar M, alBouna B, Malluhi Q. (2013). Secure outsourcing of network flow data analysis. In Big Data (Big Data Congress), 2013 IEEE International Congress On. IEEE (pp. 431-432, 71). Santa Clara, CA, USA: 10.1109/BigData.Congress.
7. Bass T. (2000). Intrusion detection systems and multisensor data fusion. Commun ACM, 43(4): 99-105. 10.1145/332051.332079.

8. Bartos K, Rehak M. (2012). Self-organized mechanism for distributed setup of multiple heterogeneous intrusion detection systems. In Self-Adaptive and Self-Organizing Systems Workshops (SASOW), IEEE sixth international conference on. IEEE, (pp. 2012:31-38. 10.1109/SASOW.2012.15). Lyon, France.
9. A. M. Kanthe, D. Simunic and R. Prasad. (2012). "Effects of Malicious Attacks in Mobile Ad-hoc Networks". IEEE International Conference on Computational Intelligence and Computing Research.
10. Yen T-F, Oprea A, Onarlioglu K, Leetham T, Robertson W, Juels A, Kirda E. (2013). Beehive: large-scale log analysis for detecting suspicious activity in enterprise networks. In Proceedings of the 29th Annual Computer Security Applications Conference ACM, (pp. 199-208. 10.1145/2523649.2523670). New Orleans, LA, USA.
11. E. Cooke, M. Bailey, Z.M.Mao, D.Watson, and F. Jahanian. (October 2004). Toward understanding distributed blackhole placement. In Proc of CM CCS Workshop on Rapid Malcode (pp. 54-64). ACM Press.
12. Y. -C. Hu and A. Perrig. (May - June 2004). "A survey of secure wireless ad hoc routing,". IEEE Security & Privacy Magazine, vol. 2, no. 3, pp. 28-39.
13. P. Papadimitratos and Z. J. Haas. (September 2003). "Secure routing: Secure data transmission in mobile ad hoc networks,". in Proceedings of the 2003 ACM Workshop on Wireless Security.
14. S. Yi, P. Naldurg, and R. Kravets,. (October 2001). "Security-aware ad hoc routing for wireless networks,". in Proceedings of the 2nd ACM International Sysmposium on Mobile Ad Hoc Networking & Computing, (pp. 299-302).
15. A.D. Wood and J.A. Stankovic. (2002). "Denial of Service in Sensor Networks,". Computer, vol.35, no.10, 2002, pp.54-62.
16. E.Shi and A.Perrig. (Dec. 2004). "Designing Secure Sensor Networks,". Wireless Commun. Mag, vol.11, no.6, pp.38-43.
17. Al-Jaroodi, J. (November 2002). "Security Issues in Wireless Mobile Ad Hoc Networks at the Network Layer,". University of Nebraska - Lincoln, Dept. of Computer Science and Engineering, Technical Report.
18. J.P. Hubaux, L. Buttyan, and S. Capkun. (Oct. 4-5, 2001). "The Quest for Security in Mobile Ad Hoc Networks,". in Proc. of the 2nd ACM International Symposium on Mobile Ad Hoc Networking and Computing (pp. 146-155). MobilHOC 2001.
19. J, F. (1994). Artificial intelligence and intrusion detection: current and future directions. In Proceedings of the 17th national computer security conference (Vol.10 pp.1-12). Baltimore, MD, USA: Citeseer.