International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

A Survey of Intrusion Detection on Spontaneous Wireless Adhoc Networks

Thangaraj E[1], Arockia Jayadhas S[2]

[1]St.Joseph College of Engineering and Technology in Tanzania, Department of Computer Science and Engineering, Dar es Salaam 11007, Tanzania

[2]St. Joseph College of Engineering and Technology in Tanzania, Department of Electronics and Communication Engineering, Dar es Salaam 11007, Tanzania

Abstract: ***This paper suggesting a sheltered protocol for spontaneous wireless ad hoc networks which uses public and private key that has trust in users in order to exchange the initial data and to exchange the data storage, manipulation, presentation, communication and other capabilities by encrypt such network services. While a sequence of operations that ensure protection of data used with a sheltered protocol, it provides secure delivery of message between network users and monitors the activities by using IDS. Most of the protocol takes network creation, management and protocol messages for building a network with spontaneous, so that it meets the requirement in a physical space in order to make use of services such as communication in group and security. The members who make up this community may vary at any specific time (users may join or leave at will), also offering self-configured sheltered protocol that is able to create the network and share networks secure services. These instructions provide you guidelines for preparing papers for International Journal of Science & Research (IJSR). Use this document as a template and as an instruction set. Please submit your manuscript by IJSR Online Submission Module.***

Keywords: DNS, IDC, IDS, NIDS

1. Introduction

Intrusion detection (ID) is a type of security management system for computers and networks. An ID system collects and analyzes the information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organization) and misuse (attacks from within the organization). ID uses vulnerability assessment (sometimes referred to as scanning), which one is the technology developed to assess the security of a computer system or network. Why do we need Intrusion Detection?

An intrusion detection system (IDS) monitors network traffic and looking after the suspicious activity and alerts the system or network administrator. In special cases the IDS may also respond to anomalous or malicious traffic by taking action such as blocking the user or source IP address from accessing the network. IDS come in a variety of “flavors” and approach the goal of detecting suspicious traffic in different ways. There are network based (NIDS) and host based (HIDS) intrusion detection systems. There are IDS that detect based on monitoring for specific signatures of known threats- similar to the way antivirus software typically detects and protects against malware- and there are some IDS that detect oriented on comparing traffic patterns against a baseline and looking for anomalies. There are IDS that simply that monitor and alert and there are some IDS that perform an action or actions in response to a detected threat. We will cover each of these shortly.

2. Related Works

One of the main issues that difference the spontaneous networks from other fixed or mobile networks is that they facilitate the integration of services and devices, setting up both the new services and the configuration parameters of the devices. It has to be done without the user intervention or interference in the operation of the network. The malfunction or unsuccessful of one of the devices or services does not compromise the viability of the community. Any information’s being used by the community which malfunction is automatically released and the service is deregistered. A spontaneous network enables a group of devices to work together collaboratively while they are located very close to each other with a minimum interaction. It can be used for sharing information’s and internet services. But, we should take into account the limitation of the resources of the devices. Just one of the nodes has to be connected to Internet to share its connection and its resources to the whole network. Caching technical methods are demanded in order to avoid the overload of the nodes. Moreover, configuration with a minimal interaction from the user and security on the communication should be connected. There are many application areas for ad hoc spontaneous networks: industrial (communication between sensors, robots, and digital networks), business (meeting, stock control, etc.), military (hard and hostile environments), and teaching. The usage of environments in which these networks can be applied is wide and may include conference services and other "ubiquitous computing" applications at home or office.

3. Security Goals

Security is an important impact for ad hoc networks, particularly for the security-sensitive applications. The ad hoc network, we having following securing attributes namely: availability, confidential, integrity, authentication and non-repudiation.

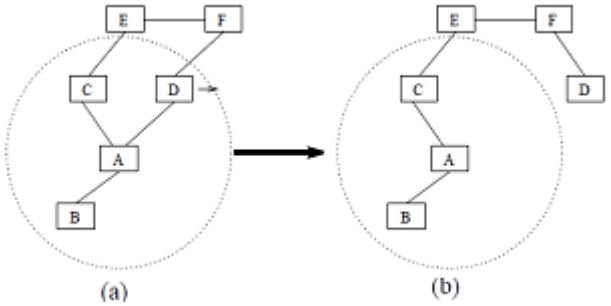

Figure 1: Topology change in ad hoc networks

Systems A, B, C, D, E, and F constitute an ad hoc network. The circle follows the radio range of system A. The network basically has the topology in (a). When system D goes out of the radio range of A, the network topology convert to the one in (b).Availability checks the survivability of network services in spite of denial of service attacks. A reject of service attack could be passed at any layer of an ad hoc network. In the physical and media access control layers, an adversary could employ congestion to interfere with communication on physical Medias. In the network layer, an adversary might disrupt the routing protocol and disconnect the network. On the upper layers, an adversary could bring down upper-level services. One such target is the key management service for the main service for any security framework.

Confidentiality checks that corresponding information is never disconnected to unauthorized entities. Network transmission of sensitive message, such as strategic or tactical military information, requires confidentiality. Leak of such message to enemies might have devastating consequences. Routing information must remain confidential in certain cases, because the information can be valuable for enemies to identify and to locate their targets in a battlefield.

Integrity guarantees that a message being exchanged is won't tainted at any time. A message could be corrupted because of begin failures, such as radio propagation impairment, or because of malicious attacks in the network.

Authentication enables a system to ensure the identity of the peer system it is communicating with or without authentication, an adversary could masquerade a system, thus gaining unauthorized access to resource and sensitive information and interfering with the operation of other systems. Finally, non-repudiation checks that the origin of a message cannot reject having to pass the message. Non repudiation is useful for detection and isolation of compromised system. When a system A receives a more message from a system B, non-repudiation allows A to accuse B using this message and to convince other system that B is compromised. A set of operations that checks the protection of data to use with a communications protocol, it gives the secure delivery of data between two parties.

4. Types of Intrusion Detection

4.1NIDS

Network Intrusion Detection Systems are used at a strategic point or points within the network to monitor traffic to and from all devices on the network. Ideally you would scan all inbound and out of range traffic, however doing so might create a bottleneck that would impair the overall speed of the network.

4.2. HIDS

Host Intrusion Detection Systems are run on individual hosts or devices on the network. A HIDS monitors the inbound and outbound packets from the device only and will alert the user or administrator of suspicious activity is detected

4.3. Signature Based

A signature based IDS will looking packets on the network and compares them against a database of signatures or characteristics from known malicious threats. This is similar to the way most of all antivirus software detects malware. This issue is that there will be a delay between a new threat being discovered in the wild and the signature for detecting that threat being applied to your IDS. During that particular delay time your IDS would be not able to detect the new threat.

4.4. Anomaly Based

An IDS which is anomaly based will monitor network traffic and compare it against an established baseline. The baseline will identify what is "normal" for that network- what sort of bandwidth is generally used, which protocols can be used, what ports and devices normally connect to each other- and alert the administrator or user when traffic is detected which is anomalous, or pointedly different than the baseline.

5. Working Principles

This protocol helps to create secure spontaneous network which will be in decentralize and distributed in nature with use of different devices .The cooperation between the devices allows for service of group, communication systems and security. Spontaneous network will be created in following way.

1. Node joining
2. Service Accessing
3. Trust Chain

1. Node joining

The joining procedure depends on the IDC i.e. Identity card which is holds by the every system whether it is in network or not. The IDC contain public and private component public component is nothing but the unique name, photograph, public key, creation, and expiration time, IP. In private component contain private key which will be used for issuing certificate to valid user. When any node supposes B

wants to join existing network, it must be select the system which is in communication range to validate itself (e.g. system A) A will send its public key. Then, the system B will send its IDC signed by system A's public key. Next, A validates the received information and verifying the hash of the information in order to check that the data has not been changed. In this step, A check the trust level of B by seeing physically at B (they are physically close), depends upon whether A knows B or not. Lastly, A will send its IDC information to B (it may do so even if it decides not to trust B). This information will be signed by B's public key (which has been received on B's IDC) .B will validate A's IDC and will check and do the trust and validity in A only by integrity verification and authentication. If A does not acknowledge to the joining request, B must be select another network system (if one exists). After the authentication, B can access services, informations and other system certificates by a route involving other nodes in network. Once the system is validated then the session key which is randomly created by first system of network is then distributed to all system of network.

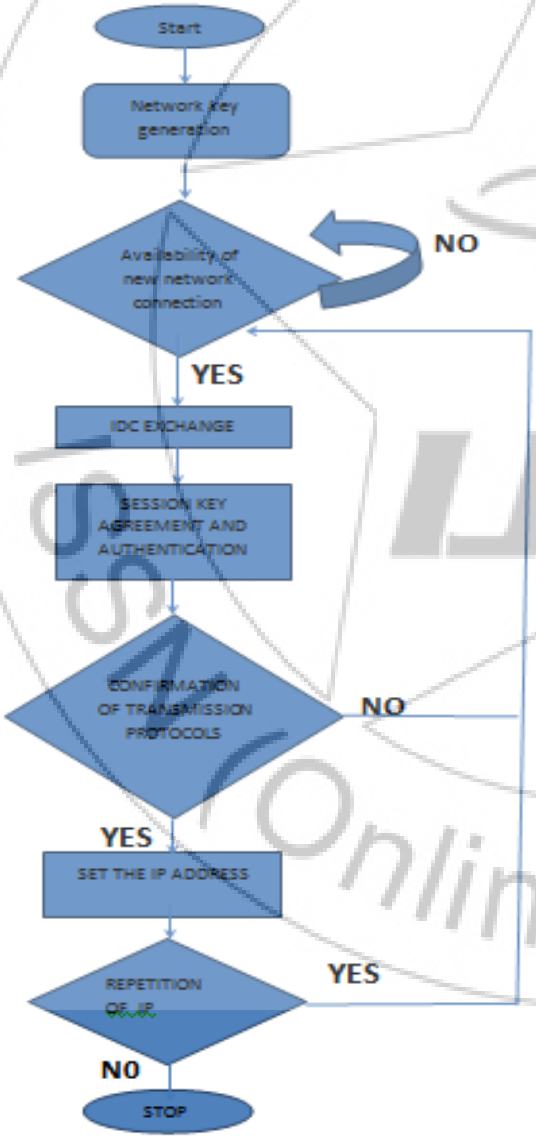

Figure 2: Joining node

The node joining procedure is combination of symmetric and asymmetric key combination process in following way. Here symmetric key is use as session key to encrypt the confidential message for that Advance Encryption standard (AES) algorithm is AES. AES require less execution time and low energy consumption where's asymmetric key cryptography is use for user authentication and session key distribution process so hence Rivest, Shamir and Adleman cryptography algorithm(RSA) is use for asymmetric key cryptography .finally IP if new node with be generated and will check for duplication. The first node in the network will be responsible for setting the global settings of the spontaneous network (SSID, session key). However, each node must configure its own data (including the first node): IP, data, port, and user information. This information will help the node to become part of the network. After this message are saving in the first node, it changes to standby mode the second node first configures its user data and security, the greeting process starts. It authenticates with the first system, the protocol relies on a sub layer protocol. The connection is created through a small-range link technology, to provide selection of nodes and ease of detection, and visual contact with the user of the node. Moreover, minimal involvement of the user is required to configure the device to establish trust. This technology also borders the scope and the consumption of participated systems. Each new system authenticates with any node in the network.

2. Service Accessing

For accessing the service the system in network has the agreement with each other .A user can ask other devices in order to know available services. Services have more numbers of parameter which are not transparent to the user and required to configure manually to manage the automatic integration tasks of network systems, for example, service agents.

Other is to manage the secure access to the services offered by the systems in the network. The fault tolerance is oriented on the routing protocol used to send message between the different users. Services provided by A is available only if there is a path to the A, if the path to system is disappear then the service is automatically gets disappear. Each system requests the services from all the other system that it trusts/ knows system in the network this differs according to types of service.

A Request to multiple systems is made through diffusion processes. The protocol prioritizes access to the message. When the message cannot be obtained through these systems, it can then ask other systems. System can also pass the requests to update network information. The acknowledge will contain the identity cards of all system in the network. The systems are replying to this request sign this data confirming the authenticity of the shipment. If it is a genuine node then its validity is also confirmed, since trusted systems have been responsible for validating their previous certificates. Using this network, any type of service or application would be applied securely.

3. Trust Chain

There are only two trust levels in the system, either trust or does not trust a Node either trusts or does not trust another system B. The user interface of application installed in the

device asks B to trust A when it receives the validated IDC from A. Trust relationship can be asymmetric. If system A did not find trust level with system B directly, it can be connected through trusted chains network, e.g., if a system trusts C system and C system trusts B system, then a system may trust B system. Trust level ought to be changing over time depending on the system characteristics. Thus, system A may decide not to trust system B although A still trusts C and C trusts B. It would also stop trusting if it generates that previous trust chain does not exist anytime.

6. Authentication Procedure

The authentication process for new device B is shown in Figure. 2. The receiver system A validates the received information and sends a broadcast message to B to check if these informations are not used in the network (like the IP address). This IP address checking packet is sent randomly two times in order to avoid simultaneous checks and reach all devices.

When the authentication device receives the IP checking packet, it sends the authentication acknowledgement to the new device. If any above step is wrong, an error message is sent to the new device when the system is authenticated, it can be perform several network operation and configuration task some of them are transparent to user

7. Session Key Revocation

The spontaneous network is usually connected for a limited period of time, which is usually not for the longer time .The user certificate has an its own expiration time. After expiration time taken, the user should authenticate with the device in the network. Otherwise, the Device will prevent the Session key has an expiration time, so the session key should repeal periodically. A system that leaves the spontaneous network will keeping the session key until it expires. It will let the user back to the network if it has joined previously. However, if a system is disconnected from the network when the session key has been renewed, it will unable to become the part of the network until it is authenticated again with someone system from the network. The session key is having three parts: (i) session key creation date/time (Fc), (ii) session key initial expiration time/date (Fe1), and (iii) the session key (Ks). The lifetime of the session key is Til = Fe1 -Fc. When a system receives the session key, it will reproduce the expiration time/date of the key by using the session key initial expiration date/time. The expiration time/date(Fe2) is the session key that initial expiration time/date plus a random number that ranges from 1 minute to the maximum predicted duration time of the spontaneous network (this value depends on the type of spontaneous network: teaching , meeting). Fc, Fe1,Fe2, and Ks are saved in each system.

8. Proposed Framework

A spontaneous ad hoc network is type of ad hoc network that is formed in a certain time during a period of time, with independence on a central server and without the intervention of an expert user, in order to solve a problem or carry out a specific task. This network is built by several independent nodes coming together at the same time and in the same place to be able to communicate with each other. Systems are free to enter and leave the network and they could be mobile or not. Spontaneous networking happens when neighboring systems discover each other within a short period of time; however, the velocity of discovery is paid in terms of power consumption. Spontaneous networks are conceptually in a higher level of abstraction than ad hoc ones; they are basically those which seek to imitate human relationships in order to work together in groups, running on an existing technology. Their aim is the integration of services and devices in an environment which allows the provision to the user of an instant service with minimum manual intervention. The idea of spontaneous networks was introduced in depth by Laura Marie et al. The main features in spontaneous networks are the following.

1. Network boundaries are poorly defined.
2. The network is not planned.
3. Hosts are not pre-configured.
4. There are not any central servers.
5. Users are not experts.

In these classifications of network the configuration services needed depend mainly on the network size, the nature of the participating nodes, and the applications that have to be carried out.

9. Conclusion

Our main objective is to enable secured spontaneous networking in a user friendly way. In the beginning configuration and security parameter exchange we chose to make use of a symmetric and asymmetric key cryptography, which helped us to cope with the major Issues of spontaneous networking. We display the process of protocol that allows the creation and management of a spontaneous wireless ad hoc network. It imitates attitudes of human relationships. It is based on a social network .Thus; each user will work to maintain the network, to provide message to the other network users and improve the services offered. We have proposed some procedures for self-configuration: like assigning unique IP address to each device, managing DNS and the accessing the services automatically. It is also provide the more no.of security to data sharing with intrusion detection.

10. Acknowledgement

I would like to thank my mother and brother for their valuable encouragement and special thanks to Mr. Godwin Jam and the staff members from the St. Joseph University for their Technical Support to us.

References

[1] Amandeep Verma1 and Manpreet Singh Gujral “Trust Oriented Secure Ad hoc Networks: A Generic Framework” (2013).

[2] Bhalaji N., Sivaramkrishnan A. R., Banerjee S., Sundar V. and Shanmugam A., "Trust Enhanced Dynamic Source Routing Protocol for Adhoc Networks", World Academy of Science, Engineering and Technology, pp. 1074-1079, 2009.
[3] Cho Jin-Hee, Swami Ananthram and Chen Ing-Ray, " A Survey on Trust Management for Mobile Ad Hoc Networks,"IEEE Communications Surveys and Tutorials, vol. 13, no. 4, pp. 562-583, 2011
[4] Giuseppe Anastasi and Eleonora Borgia, Marco Conti, Enrico Gregori "IEEE 802.11b Ad Hoc Networks: Performance Measurements"(2013).
[5] Grandison Tyrone and Sloman Morris, "A Survey of Trust in Internet Applications," IEEE Communications Surveys and Tutorials, vol. 3, issue 4, pp. 2-16, 2000
[6] Liu, J. Xu, N. Antonopoulos, J. Li, and K. Wu, "Adaptive Service Discovery on Service-Oriented and Spontaneous Sensor Systems," Ad hoc and Sensor Wireless Networks, vol. 14, nos. 1/2,pp. 107-132,2012.
[7] Nikhil Varghane, Prof. Bhakti Kurade, and Prof. Chandradas Pote, "Intrusion Detection, Secure Protocol & Network Creation for Spontaneous Wireless AD HOC Networks", Proceedings of the International Journal of Computer Science and Mobile Computing , (2014).
[8] PayalA.Pawade #1, V.T.Gaikwad "Authenticating Protocol for Spontaneous WirelessAd HocNetworks", International Journal of Computer Science and Management Research Vol 2 Issue 5 May 2013 ISSN 2278-733X..
[9] Q. H. Mahmoud and P. Popowicz, "Toward a Framework for the Discovery and Acquisition of Mobile Applications", Proceedings of the Ninth International Conference on Mobile Business and Ninth Global Mobility Roundtable, (2010).
[10] Raquel Lacuesta, Jaime Lloret, Senior Member, IEEE, Miguel Garcia, Student Member, IEEE, and Lourdes Pen˜ alver-" A Secure Protocol for Spontaneous Wireless Ad Hoc Networks Creation",ieee transactions on parallel and distributed systems, (2013)
[11] S. Capkun, L. Buttyan, and J. Hubaux, "Sector: Secure Tracking of Node Encounters in Multi-hop Wireless Networks. Proc. of the ACM Workshop on Security of Ad Hoc and Sensor Networks," 2003.
[12] Y. Hu, A. Perrig, and D. Johnson, "Ariadne: A Secure On-Demand Routing for Ad Hoc Networks," Proc. of MobiCom 2002, Atlanta, 2002.

Author Profile

Mr. Thangaraj E. received the M. Tech in Computer Science and Engineering at Dr. M.G.R Educational and Research Institute University in Chennai and B. E degree in Computer Science and Engineering at Madurai Kamaraj University in Madurai. Presently he is working as a lecturer in ST. Joseph College of Engineering and Technology in Tanzania for the past 3 years. His area of interest is networking and cloud computing.

Mr. Arockia Jayadhas received the M.Tech in Applied Electronics and B. E in Electronics and Communication Engineering in Sathyabama University in Chennai. Presently he is working as a lecturer in ST. Joseph College of Engineering and Technology in Tanzania for the past 3 years. His area of interest is networking and Digital Image Processing.