ENHANCED SECURITY IN SPONTANEOUS WIRELESS AD HOC NETWORKS WITH INTRUSION DETECTION

Vani Menon C[1], Mary Mareena P V[2]

[1]*M.Tech Student, Department of CSE, NCERC, Kerala, India*
[2]*Assistant Professor, Department of CSE, NCERC, Kerala, India*

Abstract

Spontaneous ad hoc network is created by a set of nodes placed together in the close region for some cooperative activity. A complete self-configured secure protocol uses the human interactions related with the activity to establish a basic service and security infrastructure. In order to achieve this requirement, authenticating the individual node as they come in the range of wireless network is needed. The secure protocol uses a hybrid symmetric or asymmetric scheme and the trust among users. The design of the protocol permits sharing resources and offering new services between users in a secure environment. Malicious nodes send or forward the data, which may disrupt the communication. The nodes in the network need to find out the malicious node. This paper describes a secure protocol for the network. The main focus of this paper is on the network management, security analysis of the system and an intrusion detection mechanism for spontaneous ad hoc network.

Keywords: *spontaneous wireless network, secure protocol, public key, private key*

----------***----------

1. INTRODUCTION

Mobile ad hoc network (MANET) is a dynamic wireless network that offers significant advantages that appear very promising to suit challenging requirements of novel applications. MANETs support spontaneous networking and that has turned mobile ad hoc networking into a hot topic in research. Spontaneous wireless networks are regarded as interesting solutions to extend wireless networks disadvantaged by increasingly heavy smart phone data communications. In addition, spontaneous networks can extend the reach of wireless internet access without any fixed infrastructure. In this network, the nodes establish routing among themselves dynamically to form their own network as shown in Figure-1.

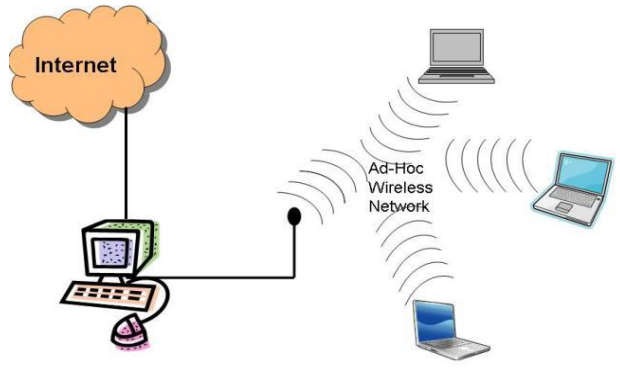

Fig -1: Spontaneous network model

The networked devices presently run towards infinity and the administration effort for managing these devices also have increased. Spontaneous networks can reduce the effort to integrate devices and services into network environments with the intention to have instant service availability with no dependence on a central server. A spontaneous network is defined as an ad hoc network that is built spontaneously as devices connect. This network enables a natural form of wireless computing when humans interact with each other. A Spontaneous Wireless Ad Hoc network is formed, when two or more nodes come together in the closed area for communication and to share the resources for the duration of limited time. Users are automatically connected to the network, establish their needed channels and share services. The main purpose is to facilitate secured spontaneous networking in a user friendly way. Automatic device integration into network environments enables the device to communicate with others.

The requirements for the configuration services of these networks depend mainly on size of the network, the nature of cooperation among nodes and on the applications that are running. The tasks to be carried out in the configuration of these types of networks include the identification of nodes and their authorization, address assignment, service name and security. Nodes are free to join or leave the network as it might be susceptible to attack if nodes involved are not trusted. Security has become a primary concern in order to provide confined communication in a dynamic environment.

Ad hoc spontaneous networks require a protocol which adapts to any number of dissimilar nodes. The network and protocol based on user trust can establish a secured self configured environment for data sharing and resources and services distribution among users. By building a trust network and on the user service needs, security is established. This enables to obtain a distributed certification authority which is necessary to build trust networks. The network permits users to connect because it belongs to someone who knows it. We used to concern asymmetric cryptography where every device has a public-private key pair for discovering the device and also symmetric cryptography to share session keys among nodes. Authentication and trust phase is used to solve the security issues. There are unidentified users, because validity and privacy depends on user identification [1].

In wireless communication technologies, security has a primary concern in effort to give secure communication in a hostile wireless environment. Nodes can be easily captured and fake messages can be injected into the network. Several approaches for securing communication in ad hoc networks have been proposed. Here the protocol based on user trust offers security while requiring less energy. In order to attain an acceptable level of security without affecting their efficiency, intrusion detection approach is proposed. This mechanism can extend the network security by finding out intruders. Furthermore, stream cipher introduced to enhance the performance when transferring data among nodes. Salsa20 offers a much better speed security profile than the block cipher AES [2] [3]. Stream ciphers have limited or no error propagation whose block diagram is shown in Figure-2 with the plaintext and the corresponding encrypted cipher text. The cipher text is the xor of the plaintext and the stream, where stream is determined by the key and nonce. In Salsa20 the reduced round ciphers provides an attractive option for users who considers more importance to speed.

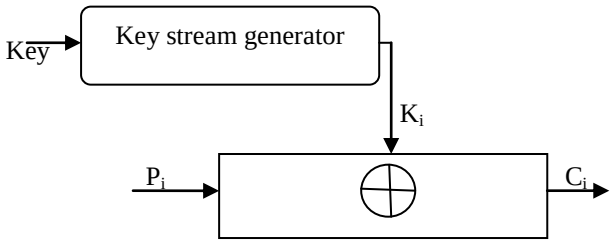

Fig -2: Stream cipher

2. RELATED WORK

An ad hoc network must operate independent of an access point infrastructure, whereas still offering essential administrative services to support applications. In an ad hoc environment, nodes have to cooperate to provide the functionality of group communication. Security in fixed network relies on a central server to certify nodes that want to communicate with each other but this is not the case with spontaneous network. The phase of authentication and trust is a fundamental topic in the environment of security in spontaneous networks [4].

The methods used earlier enable the users to get the service required without any external infrastructure. The nodes participating may not be able to execute routing and security protocols. The design and use of adaptive routing and security mechanisms is necessary for any type of devices and scenarios. It is difficult to manage the dynamic networks which are with flexible memberships, group and distributed signatures. Key exchange mechanisms for user authentication and node authorization are required to obtain a reliable communication. The methods adopted are not enough for spontaneous networks since they need configuration to perform initially.

Zhu et al. [5] developed a scalable and light-weight secure protocol for ad hoc networks. Most of the routing protocols for ad hoc networks do not apply network access control. This causes the networks susceptible to resource consumption attacks where a malicious node injects erroneous routing updates into the network with the goal of paralyzing the network. In order to prevent such attacks, it is necessary that a node joining ad hoc network employs some authentication mechanisms. Using Lightweight Hop by Hop Authentication protocol trust relationship with its neighbours can be bootstrapped.

Backstrom et al. [6] developed the first real spontaneous network using the Jini technology that offers services dynamically. New units can be easily added and makes possible to connect any device to the network irrespective of the operating system. A contract is initiated when the service provider unit joined the network and the duration of the service depends on the contract. The evolved technologies like Jini can ensure interoperability between different systems, but this is not spontaneous.

Untz et al. [7] proposed a lightweight interconnection protocol appropriate for spontaneous edge networks. For spontaneous edge networks, here it proposed and implemented Lilith which is a prototype of an interconnection node. The main objective is to support TCP or IP applications without configuration. To allow different communication paths on a per flow basis, it uses Multi protocol label switching. It presents seamless switching between operational and back-up paths, and the information will reach on destination reachability. Load balancing or traffic isolation for different QoS classes is provided through multiple paths. The wireless spontaneous network is of dynamic topology which causes routes to frequently appear and disappear. This can be solved by Label Switched Paths which enable the nodes to detect broken paths. But it does not have any security mechanisms.

Danzeisen et al. [8] apply Wireless Encryption Protocol (WEP), the regular security mechanism used in Wireless LANs. Building spontaneous networks between two or more nodes for communication was enabled by wireless communication technology. It is easy for the formation of spontaneous networks among heterogeneous node with cellular framework. Communication channel uses security parameters which depend on a specific technology. In Wireless LAN, wireless encryption protocol is available but it is more susceptible to hacking attacks.

Czerwinski et al. [9] introduced an architecture and implementation of a secure Service Discovery Service (SDS). Clients as well as Service providers use SDS to create complex queries for locating these services and to advertise complex descriptions of existing running services respectively. It facilitates the network enabled devices to discover available. The core component of secure service discovery service is security and, communications are both encrypted and authenticated. Certificate authority signs certificates, whose public key is known to everyone. The components include clients which want to discover services that are running in the network and servers respond to client queries. To control the access to service information, it uses a hybrid access control list.

3. SECURITY IN SPONTANEOUS NETWORK

A security protocol based on trust permits the creation and management of distributed and decentralized spontaneous networks with little interference from the user, and the incorporation of different devices. The infrastructure less network is aimed to encourage a wireless interaction. Because wireless interaction depends on physical proximity, it imitates the way humans communicate. The following steps must follow when a device joins the network.

1. Join the device into the network
   (a) Agree the broadcast protocol and speed.
   (b)Configure IP address, routing information and other type of information
2. Discover services and resources shared by the devices
   (a) Update the list of available services and resources
   (b) Share the services discovered
3. Access to the service offered by the devices
   (a) Handle the automatic configuration tasks and security access to the services
   (b) Joining and leaving a network have to be managed
4. Cooperative tasks
   (a) Cooperation of various members within the intranet
   (b) With other communities on the internet

Spontaneous networks imitate human relations which are taken into account for the security. Spontaneous ad hoc networks have many applications in the areas include industrial, business, military and teaching. It can be used during emergency situations in order to establish communication fast and reliably. Secure communication is guaranteed with cryptographic techniques. The requirements of security in spontaneous networks are the same as used in traditional networks such as privacy, integrity, verification, confidentiality and availability [10], [11].

3.1 Network Creation

The network is created using the information provided by the users. The establishment of a network allows the devices to communicate. It involves the automatic configuration of logical and physical parameters. The system is purely based on the use of an Identity Card (IDC) and a certificate. The IDC consists of public and private components for the operation. The public component consists of a Logical Identity (LID), which is unique for each node participating. LID consists of information such as name, picture or other type of user identification. It also contains public and private keys of the user. The public key is sent to other users. The creation and expiration date, IP proposed by the user and user signature generated using the Secure Hash Algorithm (SHA-1) are the other type of information included. Private key is included in the private component. Central Certification authority is not required to validate IDC. It is done by any of the trusted nodes. The exchange of IDC among nodes grows the trusted network.

When a node wants to make communication with another node and it does not have that node's certificate, it is possible to requests from its trusted nodes. The system will validate the data after receiving the certificate. If the data is correct, then it will sign as a valid node. Every node can make requests as well as serve requests for authentication or information from other nodes. The nodes can act as clients as well as servers at the same time

Spontaneous network is created by the first node as shown in Figure-3 and generates a session key arbitrarily, which will be shared with the new nodes coming after the verification phase. Network security and user data are configured by the second node and authenticates against the first node. Additional nodes authenticates with any other node in the network. A node which joins onto a network must go through some phases: verification and authorization of node, session key agreement, transmission protocol and speed, IP address checking and routing.

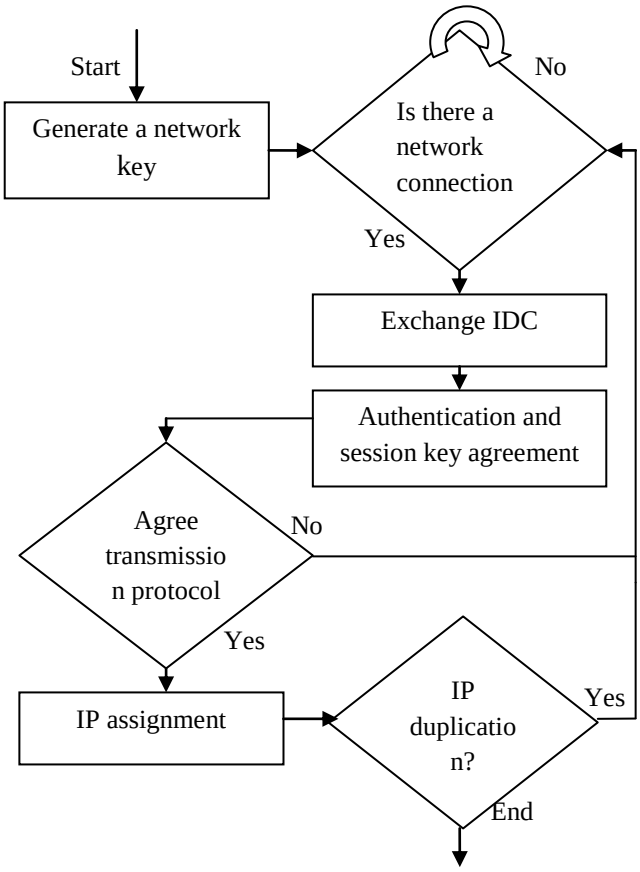

Fig -3: Network creation

Spontaneous network is created by the first node as shown in Fig. 2 and generates a session key arbitrarily, which will be shared with the new nodes coming after the verification phase. Network security and user data are configured by the second node and authenticates against the first node. Additional nodes authenticates with any other node in the network. The nodes can act as clients as well as servers at the same time.

3.2 Authentication Control

After a node joined onto the network, it sends an authentication message with its LID to its neighbor nodes. When the receiver node receives the message, it validates the received data in order to check that the data has not been already used in the network. It sends a broadcast message to other nodes present in the network to recheck that the data has not been used. If no such data present, then the node is validated and thus gets trusted. The trusted node's data is saved which then can perform several tasks. The tasks include display and modify the trust of the nodes, update the information, process the authentication request, reply and forward an information request, send data to nodes and leave the network.

3.3 Protocol Implementation

Security in the network depends on the symmetric and asymmetric key encryption mechanisms. Session key generated is used to encrypt the confidential messages among trust nodes. The algorithm used for the symmetric encryption scheme is Advanced Encryption Standard whereas for asymmetric key scheme is Rivest, Shamir and Adleman. Session key and node authentication process are distributed using asymmetric key encryption.

User only determines whether have to build a network or to join in an existing one once validation is completed. The node that wants to join a spontaneous network begins the procedure by sending a Discovery request packet to the destinations. The packet contains the LID of the sending node. The receiving packet contains the LID and IP address of the destination. The data received is used to study the chosen device to authenticate. Authentication request and reply packets, IP and e-mail checking packets are used for device authentication.

3.4 Session Key Revocation

The certificate of a node has an expiration time. The node must authenticate with the device after this session or else, the device is blocked. The session key is kept by the node until it leaves the network. The spontaneous network is typically arranged for a reduced time slot, which is usually not very extensive. When a node is left from the network during the period of time when the session key has been renewed, it will not be capable to access the network until it is authenticated again with some node present in the network. When the session key is about to expire, it sends a broadcast message to other nodes and not all nodes leave from the network at the same time.

3.5 Confidential Data Sharing

In a spontaneous network, when a node has to send data to another node or device, it is possible to send the data to either a single node or to all nodes. All the nodes can receive data only if it is sent in plaintext whereas a single node can receive the ciphered data. When the node received the data, it has to decrypt it with the model of encryption used by the source node. By session key generation, the data is distributed between two trusted users and encrypting their files. The user can access the resource only with the encrypted key if the user has the privilege to the resource sent. There are several options provided with the nodes to send the data. It can be sent symmetrically or asymmetrically encrypted, or as unencrypted which chosen by the sender.

4. PROPOSED SYSTEM

Intrusion Detection mechanism is introduced in order to achieve an acceptable security level in spontaneous ad hoc networks. The trust based approach along with the intrusion

detection mechanism enhances the security services that are required by the users. Encryption and authentication are normally the first level of security when an intrusion takes place. Secure Hash Algorithm is used to generate the digital signature on the encrypted data. And verifying the signature is done by the node receiving data. If the data are identical, the receiver node accepts the data, otherwise the data has been tampered. An alert about the intruder is then given to the nodes and thus they can avoid the paths that include compromised nodes. The proposed system of Intrusion Detection is shown in Figure-4.

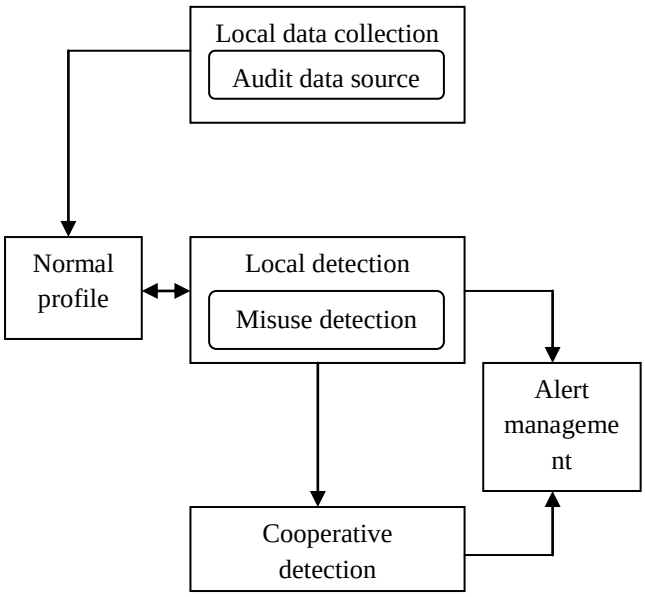

Fig -4: Proposed system of Intrusion Detection

5. EXPERIMENTAL RESULTS

Average computation time (in milliseconds) has been used to compare the performance of algorithms. Salsa20 provides consistent high speed in a wide variety of applications. The performance of the current approach was compared on the basis of the time required for the packet size to be transmitted which is shown in Figure-5. In this the packet size varies from 1 MB to 3 MB. It can be seen that the encryption scheme by using salsa20 in the secure protocol for spontaneous network has the lower execution time compared to other symmetric and asymmetric algorithms.

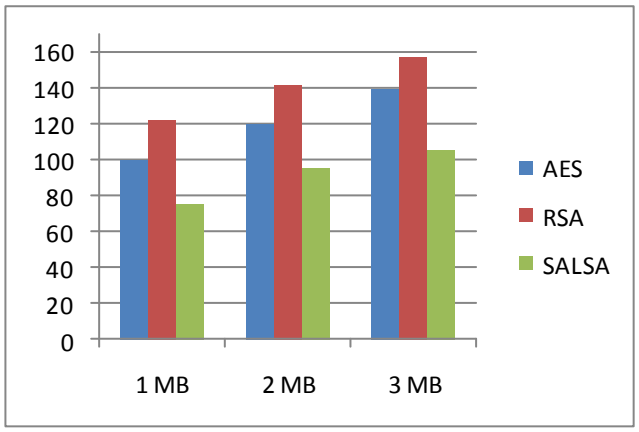

Fig -5: Performance evaluation

6. CONCLUSIONS

The design of the protocol permits secure communication among nodes in a spontaneous wireless ad hoc network. Human relations approach is used in the work done. These networks are developed to accomplish a task on a limited period of time and space. All the nodes need to cooperate for the configuration and management of the network. The devices share the required information to be trusted eventually they gain access to the network. The different users present in the network offers various resources which can be accessed by all other users in the network. It is not necessary for the devices to keep the public keys of the network and information within it. A unique IP address needs to be assigned to each device in order to get configured. It is suitable to be used in resource constrained devices. Security schemes are included using cryptographic techniques. The secure protocol allows confidential data sharing among trusted nodes. And the intrusion detection approach protects the network and enhancing the level of security in ad hoc networks.

REFERENCES

[1]. Raquel Lacuesta, Jaime Lloret, Miguel Garcia, and Lourdes Penalver,"A Secure Protocol for Spontaneous Wireless Ad Hoc Networks Creation," IEEETransactions on Parallel and Distributed Systems, Vol. 24, No. 4, April 2013.

[2]. D. J. Bernstein, "The Salsa20 Stream Cipher," SKEW, http://cr.yp.to/snuffle.html, Accessed April 2013

[3]. D. J. Bernstein, "The Salsa20 family of stream ciphers," New Stream Cipher Designs, LNCS vol. 4986, pp. 84-97, Springer, Heidelberg, 2008

[4]. L.M. Feeney, B. Ahlgren, and A. Westerlund, "Spontaneous Networking: An Application- Oriented Approach to Ad-hoc Networking," IEEE Comm.Magazine, vol. 39, no. 6, pp. 176- 181, June 2001.

[5]. S. Zhu, S. Xu, S. Setia, and S. Jajodia, "LHAP: A Lightweight Hop by-Hop Authentication Protocol For Ad-Hoc

Networks," Ad Hoc Networks J., pp. 567-585, vol. 4, no. 5, Sept. 2006.
[6]. J. Backstrom and S. Nadjim-Tehrani, " Design of a Contact Service in a Jini-Based Spontaneous Network," Proc. Int'l Conf. and Exhibits on the Convergence of IT and Comm., August 2001.
[7]. V. Untz, M. Heusse, F. Rousseau, and A. Duda, "Lilith: an Interconnection Architecture Based on Label Switching for Spontaneous Edge Networks," Proc. First Ann. Int'l Conf. Mobile and Ubiquitous Systems: Networking and Services (Mobiquitous '04), August 2001.
[8]. M. Danzeisen, T. Braun, S. Winiker, D. Rodellar,"Implementation of a Cellular Framework for Spontaneous Network Establishment," Proc. IEEE Wireless Comm. And Networking Conf. (WCNC '05), March 2005.
[9]. S.E. Czerwinski, B.Y. Zhao, T.D. Hodes, A.D. Joseph, and R.H., "An Architecture for a Secure Service Discovery Service," Proc. ACM/IEEE MobiCom, Aug. 1999.
[10]. R. Lacuesta, J. Lloret, M. Garcia, and L.Penalver,"A Spontaneous Ad-Hoc Network to Share WWW Access," EURASIP J. Wireless Comm. and Networking, vol. 2010, article 18, 2010.
[11]. Payal A.Pawade and V.T.Gaikwad "Authenticating Protocol for Spontaneous Wireless Ad Hoc Networks", International Journal of Computer Science and Management Research, vol.2, Issue-5, May 2013.