Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 2, February 2014, pg.389 – 394

RESEARCH ARTICLE

Intrusion Detection, Secure Protocol & Network Creation for Spontaneous Wireless AD HOC Network

Nikhil Varghane[1], Prof. Bhakti Kurade[2], Prof. Chandradas Pote[3]

[1]Computer Science and Engineering, G.H. Raisoni Academy Of Engineering, India
[2]Computer Science and Engineering, G.H. Raisoni Academy Of Engineering, India
[3]Computer Science and Engineering, Priyadarshini College Of Engineering, India
[1] n.varghane@gmail.com; [2] Bhakti.Kurade@Raisoni.net

Abstract— Fundamental aspect in wireless network creation & wireless communication is use of security so this paper proposing a secure protocol for spontaneous wireless ad hoc networks which uses an hybrid public ,private key scheme and the trust between users in order to exchange the initial data and to exchange the secret keys that will be used to encrypt the data. The protocol offers Network creation, protocol messages, and network management communication. We presenting self-configured secure protocol that is able to create the network and share networks secure services. The network allows sharing resources and new services among users in a secure environment. Our proposal has been implemented in order to test the protocol procedure and working. Finally, we compare the protocol with other spontaneous ad hoc network protocols in order to highlight its features and we provide a security analysis of the system. A Spontaneous ad-hoc network is a complete self-configured secure protocol which is able to create the network and share secure services without any previous setup. The network permits sharing resources and offering new services among users in a securely. The protocol contains all functionality required to operate without any outer support. Design of a protocol permits the creation and management of a spontaneous wireless ad hoc network

Keywords— public key; private key; cryptography; secure protocol; spontaneous network; wireless ad hoc networks; peer to peer network.

I. INTRODUCTION

During the last few years, wireless and mobile communication networks have quickly developed and are widely used. A mobile ad hoc network is a multi-hop wireless network formed by a collection of mobile nodes without the intervention of fixed infrastructure Mobile Ad hoc network (MANET) is a group of wireless nodes that form a network without support of any kind of network infrastructure.

Some features of MANET are as follows:

1. Host movement frequent.
2. Topology change frequent.
3. No cellular infrastructure.
4. Multi-hop wireless links.
5. Data must be routed via intermediate nodes.

Though MANET is good options over network which are depend on infrastructure, it has some challenges. They are, first, the network must operate independent of an access point infrastructure, even though the nodes connected each other rapidly and their connectivity changes unpredictably. Second is network must operate independent of a pre setup or centrally manage network infrastructure, providing administrative services support to applications. And third, routing in MANET is done by some routing protocol like DSDV or AODV, DSR. To achieve a reliable connectivity and node authentication in mobile ad hoc networks, key exchange mechanisms for node authentication and user authentication are needed security methods such as security methods such as pre-distribution key algorithms, symmetric and asymmetric algorithms, intermediate node based methods, and hybrid methods. Spontaneous networking is solution to these problems of MANET which is based on human communication. In human communication model, people come together form a group and start talking or communicating with each other by sharing their views, information and many things. During this eye to eye communication anybody can talk, join the group or leave the group without getting any permission. There is not any central organizer. But the problem is, if someone leaks any confidential information to other person therefore security is very important. Spontaneous networking is like human communication where a set of mobile nodes are placed together in a closed location for commutation to share recourses, services or computing time in limited period of time and in limited space. They usually have slight or no dependence on a centralized administration. Spontaneous network can be wireless or wired. We only considering wireless spontaneous network for our review. In spontaneous ad hoc network new services are added without user intervention. Failure or breakdown of any attached service or device does not compromise functionality of network. Network boundaries are poorly defined.

The network is not pre planned. Hosts are not preconfigured. There is not any central administration or server. Users are not experts. All these are features of spontaneous network. Spontaneous ad hoc network is a special kind of Mobile Ad hoc network (MANET). A major problem in mobile ad hoc networks is the management and dissemination of information. Since the mobile devices are restricted in their resources, a fully replication of information will not be possible. Information exchange should be restricted with respect to the spatial scope of the information and the interests of the user. Another issue is how can a user determine or specify to which information he or she is in interest. Solution to these problems is Spontaneous ad hoc network. Spontaneous network is Special case of ad hoc network. These types of networks usually have independent and distributed centralized administration. The network can be wired or wireless. Spontaneous network shares resources, services or computing time during a limited period of time and in a limited space [2]

The Important qualities in spontaneous networks are mentioned below:-
1. Network boundaries are poorly defined.
2. The network is not planned.
3. Hosts are not preconfigured.
4. There are not any central servers.
5. Users are not experts.

The main goal of spontaneous network is collaboration of service and devices at one place allowing user to have instant service without external infrastructure .this networks are implemented in mobile phones, PDA, laptops, with limited memory space and limited energy. Sensors and actuators in home and industry automation are controlled via digital networks. Security in networks must involve node cooperation, authentication, confidentiality, anonymity, and privacy also. To transfer photo require less security but to transfer confidential information require high security therefore encryption and decryption techniques are required to share information. In ad hoc networks Certificate Authority (CA) is used to authenticate the user and manage the trust. For this, CA requires high computing and time capacity and it also has to be online always. In such networks, for node authentication and user authentication a dependable media is required and there may be single point of failure. Security in spontaneous network is based on the users service needs, and to obtain a distributed certification authority it necessary to build

trust networks. The network grants users to join because it belongs to someone who knows it. Hence, the new user is well authentic by the certification authority. This allows the network to have a distributed name service and also distribution of network management.

Intrusion detection system (IDS) plays a very important role for detecting different types of attacks. The main function of intrusion detection is to protect the network, analyze and find out intrusions among audit and normal audit data, and this can be considered as a classification problem. Intrusion detection system can be classified based on detection method into two basic methods misuse detection and anomaly detection methods. The misuse detection method operates on database of known attack signatures; the system stores patterns (or signatures) of known attacks and uses them to compare with the actual actions or activity. Another process to intrusion detection is called anomaly-based intrusion detection. Anomaly detection works on the assumption that "attack behavior" differs and distinct a sufficient amount from "normal user behavior". The Anomaly detection algorithms have the advantage over a signature-based detection that they can detect novel attacks. Although Anomaly detections methods are able to detect new types of intrusions, most of these anomaly-based IDSs suffer from a high rate of false alarms due to a deficiency in their discrimination ability.

The related literature presents several security techniques Intermediate node based method [10], symmetric and asymmetric algorithm, Pre distribution key algorithm [9] and hybrid method [11] but this methods are not enough for spontaneous network because they need external authorities and initial configuration and here in this paper we are trying to propose self-configured protocol for sharing of resources and services secured data distribution among authorized users.

II. PROTOCOL WORKING

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

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

A. *Node joining*

The joining procedure depends on the IDC i.e. Identity card which is holds by every node 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 choose the node which is in communication range to validate itself (e.g. Node A) A will send its public key. Then, B will send its IDC signed by A's public key. Next, A validates the received data and verifies the hash of the message in order to check that the data has not been modified. In this step, A establishes the trust level of B by looking physically at B (they are physically close), depending on whether A knows B or not. Finally, A will send its IDC data to B (it may do so even if it decides not to trust B). This data will be signed by B's public key (which has been received on B's IDC) [4]. B will validate A's IDC and will establish the trust and validity in A only by integrity verification and authentication. If A does not reply to the joining request, B must select another network node (if one exists). After the authentication, B can access services, data and other nodes certificates by a route involving other nodes in network. Once the node is validated then session key which is randomly created by first node of network is then distributed to all nodes of network.

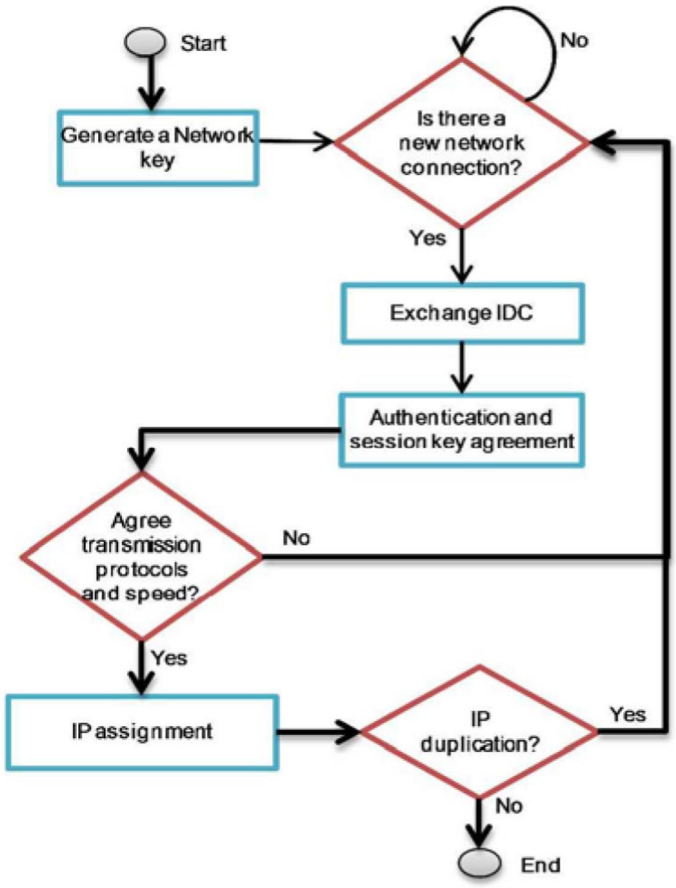

Fig. 1 Joinig the new node

The node joinig procedure is combination of symmetric and asymetric 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 ase . AES require less execution time and low energy consumption wheres asymmetric key cryptography is use for user authentication and session key distribution process so hence Rivest, Shamir and Adleman cryptoghraphy algorithm(RSA) is use for asymmetric key cryptoghraphy .finally IP pf 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 data. This information will help the node to become part of the network. After this data are saving in the first node, it changes to standby mode [5], [8]. The second node first configures its user data and security. Then, the greeting process starts. It authenticates with the first node. Our protocol relies on a sub layer protocol. The connection is created through a short-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 mainly to establish trust. This technology also borders the scope and the consumption of involved nodes. Each new node authenticates with any node in the network [7].

B. *Service Accessing*

For accessing the service the nodes in network have the agreement with each other .A user can ask other devices in order to know available services. Services have large numbers of parameter which are not transparent to user and required to configure manually. To manage the automatic integration tasks of network nodes, for example, service agents. Other is to manage secure access to the services offered by the nodes in the network. The fault tolerance is based on the routing protocol used to send information between users. Services provided by A are available only if there is a path to A, if the path to node is disappear the service is also automatically gets disappear [3]. Each node requests the services from all the other nodes that it trusts or knows nodes in the network this varies according to types of service. A request to multiple nodes is made through diffusion processes. The protocol prioritizes access to information. When the information cannot be obtained through these nodes, it can then ask

other nodes. Nodes can also send requests to update network information. The reply will contain the identity cards of all nodes in the network. The nodes replying to this request sign this data ensuring the authenticity of the shipment. If it is a trusted node then its validity is also ensured, since trusted nodes have been responsible for validating their previous certificates. Under this network, any type of service or application can be implemented securely

C. *Trust Chain*

There are only two trust levels in the system, either trust or does not trust. Node A either trusts or does not trust another node 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 node A did not establish trust level with node B directly, it can be established through trusted chains network, e.g., if A node trusts C node and C node trusts B node, then A node may trust B node. Trust level can change over time depending on the node's behavior. Thus, node A may decide not to trust node B although A still trusts C and C trusts B. It can also stop trusting if it discovers that previous trust chain does not exist anymore [1], [10].

III. AUTHENTICATION PROCEDURE

The authentication process for new device B is shown in Fig. 2. The receiver node A validates the received data and sends a broadcast message to B to check if these data 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 [9], [5]. When the authentication device receives the IP checking packet, it sends the authentication reply to the new device. If any step is wrong, an error message is sent to the new device when the node is authenticated, it is able to perform several network operation and configuration task some of them are transparent to user [3].

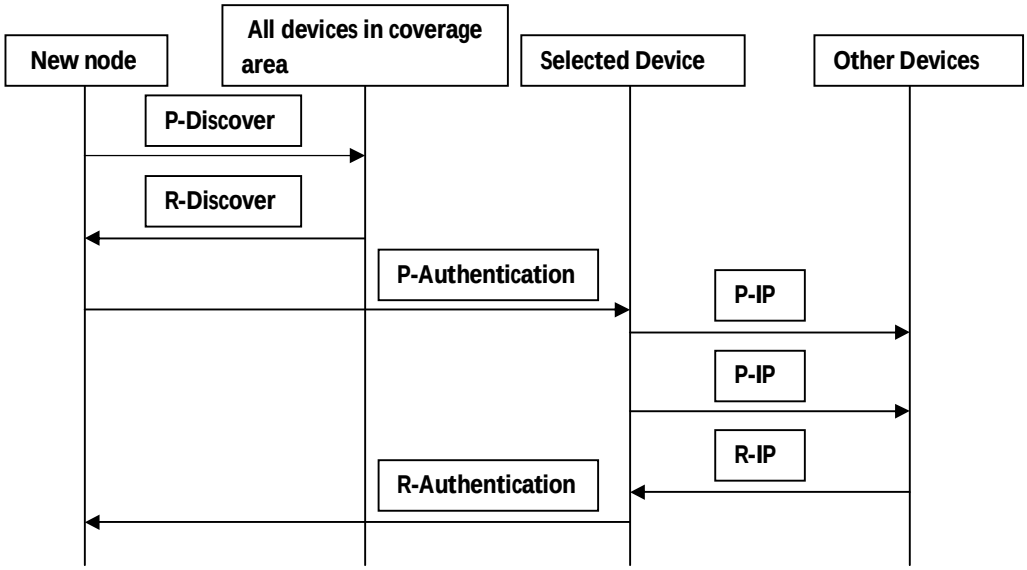

Fig. 2 Authentication Procedure

IV. SESSION KEY REVOKATION

The spontaneous network is usually established for a limited period of time, which is usually not for longer time .The user certificate has an expiration time. After expiration time, the user must authenticate with the device in network. Otherwise, the device will block. Session key has an expiration time, so session key should revoke periodically. A node that leaves the spontaneous network will keep the session key until it expires. It will let the user return to the network if it has joined previously. However, if a node is disconnected from the network when the session key has been renewed, it will not be able to become the part of network until it is authenticated again with someone node from the network. The session key is formed by three parts: session key creation date/time (Fc), session key initial expiration time/date (Fe1), and the session key (Ks). The lifetime of the session key is Til = Fe1 - Fc. When a node receives the session key, it will regenerate 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 initial expiration time/date plus a random number that ranges from 1 minute to the maximum anticipated 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

node. Session keys do not expire at a time in all nodes. This avoids network flooding initiated at a time by many nodes, when the session key is to be revoked. When node that detects expiring session key lifetime, it will send a broadcast its current time to advise other nodes that a new session key will be generated. If to node has same session key in such case the node with oldest time wins. Once the node generate session key then, node broadcast session key encrypted with the old session key to all their neighbors. Then, the receiver will save the new session key with the new initial expiration time and will replace the old session key with the new one, thus it will only be able to communicate with only updated nodes.

V. CONCLUSION

Our main objective is to enable secured spontaneous networking in a user friendly way. For the initial 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 show the process of protocol that allows the creation and management of a spontaneous wireless ad hoc network. It imitates behavior of human relationships. It is based on a social network .Thus; each user will work to maintain the network, provide information to 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 security to data sharing with intrusion detection.

REFERENCES

[1] 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, vol. 24, no. 4, april 2013.

[2]L. 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.

[3]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.

[4]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., vol. 4, no. 5, pp. 567-585, Sept. 2006.

[5]L.M. Feeney, B. Ahlgren, A. Westerlund, and A. Dunkels, "*Spontnet: Experiences in Configuring and Securing Small Ad Hoc Networks,"* Proc. Fifth Int'l Workshop Network Appliances, Oct. 2002.

[6]J. Latvakoski, D. Pakkala, and P. Paakkonen, *"A Communication Architecture for Spontaneous Systems,"* IEEE Wireless Comm.,vol. 11, no. 3, pp. 36-42, June 2004

[7]PayalA.Pawade #1, V.T.Gaikwad *"Authenticating Protocol for Spontaneous WirelessAd Hoc Networks"*,International Journal of Computer Science and Management Research Vol 2 Issue 5 May 2013 ISSN 2278-733X.

[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),Mar. 2005.

[9] 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),. 2004.

[10] R. Lacuesta and L. Pen˜ alver, *"Automatic Configuration of Ad-Hoc Networks: Establishing Unique IP Link-Local Addresses,"* Proc. Int'l Conf. Emerging Security Information, Systems and Technologies(SECURWARE '07), 2007.

[11] R. Lacuesta and L. Pen˜ alver, "*Automatic Configuration of Ad-Hoc Networks: Establishing Unique IP Link-Local Addresses*," Proc.Int'l Conf. Emerging Security Information, Systems and Technologies(SECURWARE '07), 2007.

[12] L. Herrero and R. Lacuesta, "*A Security Architecture Proposal for Spontaneous Networks*," Proc. Int'l Conf. Advances in the InternetProcessing System and Interdisciplinary Research, Oct. 2003.

