A Survey On Symmetric Key Protocol For Spontaneous Wireless Ad Hoc Network Creation

Priyanka M. Nandagawli, A.R.Tayal, Anil Jaiswal

Abstract: In this paper present a symmetric key protocol for spontaneous wireless ad hoc network creation which uses a hybrid symmetric scheme. In our proposal is a complete independent self configured network creation there is no need any fixed infrastructure as well as no need any central administrator to handle the services and share the secure data and no need any external support for handling the functionalities of the network. A spontaneous ad hoc network is complete self configured secure protocol which is able to create the independent network and share the secure services without any setup and offer the new services among users are present in the secure environment. This protocol contains all function required to operate without any external support. Design of a protocol make available the creation and management of a spontaneous wireless ad hoc network.

1. INTODUCTION:

A set of mobile terminals that are placed in a close location communicate with each other, share the resources and services or computing time during a limited period of time and a limited space forms Spontaneous ad hoc networks. These types of networks usually have independent centralized administration. They can be wired or wireless by making Spontaneous network a Special case of ad hoc network. Spontaneous ad hoc networks need well defined, effective and user-friendly security mechanisms. Tasks to be performed in this type of network include: Identity of User, their authorization, Address to be assigned, service name, safety and operation. The Significant dependency of Configuration services in spontaneous networks is on the size of the network or nature of participates Of Nodes and running applications. Intentional interactions among users who have preferred to Collaborate for some purpose is reflected by spontaneous network. It can be leveraged in order to create an ordered method for modifying the network configuration. In this type of network have limited scope in time and space. They include powerful host machines, such as laptop computers or developing high-end personal digital assistants (PDAs) and cellular phones. The features of spontaneous networks are mentioned below:-

1. The network boundaries are poorly defined.
2. The network is not properly planned.
3. The hosts are not preconfigured.
4. There are not any central servers or administrator.
5. Users are not expertise.

A spontaneous network enables the group of devices to work together and share data while they are located very close to each other with a minimum interaction. It can used to share resources and many internet services. But, we should take into account the limitation of the resources in the devices. Only once of the nodes are connected to Internet to share the connection and its resources to the all network. The caching technique is used to avoid the overload of the nodes. Moreover, configuration with a minimal interaction from the users and security over the communication should be formed. There are more application areas for ad hoc spontaneous networks: industrial (communication between sensor nodes, robotics, and digital networks), businesses (meeting, stock control, etc.), military (hard and hostile environments), and teaching. The range of environment in which those networks can be applied is wide and may conference services and other "ubiquitous computing" applications at home , office and etc. This paper also shows the design and simulation of a Model that lets optimal spontaneous network access by using the caching mechanism. We present the procedures of the nodes involve in the system, the some security algorithms implementation, and the design of the messages. Moreover, we can also include the analytical proposal and its comparison with the most similar protocols in the survey. The validation of the secure protocol is carried out through several simulations and compare with regular architectures. This proposal has been develop with the main objective of improve the communication and integration between different study centers of low-resources communities. We are use by applying asymmetric cryptography, where each device have a public key and private key, key pair for device identification and symmetric cryptography is used to share session keys between nodes. There are unidentified users because validity and privacy are based on user identification.

2. REVIEW:

The related literature survey shows several security methods such as redistribution key algorithm, symmetric and asymmetric algorithm, and intermediate node based methods but these types of methods are not suitable for the spontaneous network creation because they need a network configuration or external authorities. Existing methods propose a secure spontaneous network protocol based on the users trust which provides node authenticity integrity checking, confidentiality. We present a basic setup

- *Priyanka M. Nandagawli, G.H.R.I.E.T.W, Nagpur,* *pnandagawli2@gmail.com*
- *A.R.Tayal, Priyadarshini College Of Engg.,* *annu09in@gmail.com*
- *Anil Jaiswal, G.H.R.I.E.T.W, Nagpur,* *jaiswal.anil@gmail.com*

of the symmetric key protocol to handle the security issues; we can use the authentication stages and trust stages. In this paper also include the intrusion detection scheme for joining the new member in the network while that node are authenticate or not.

2.1 Spontaneous network:

2.1.1 Network Overview:

Our protocol which allows creating the independent and decentralized spontaneous networks. The network member services vary because the members at any time join or leave the network. Spontaneous network should complete the following steps to create the network.

2.1.1.1 Step 1: Joining Procedure:

The system is based on the identity card and user's certifiacate.The identity card which may contain the public-private components. The public component can contain the logical identity (LID).This logical identity is unique for each user and allows node to identify it. In this contain the information about the users such a as name, address, photograph etc. and the private For management of the security in the network is based on public key infrastructure and symmetric key encryption scheme. The public key is used as a session key to encrypt the confidential message between trust nodes.

2.1.1.2 Step 2: Service Discovery:

We can create the spontaneous ad hoc network there is no need any central server. In that nodes can discover the available services of the other nodes.

2.1.1.3 Step 3:

Establishing trusted chain and changing trust level: In this step we can create the trusted chain for example: if X trusts Z and Z trusts Y then X may trusts Y. The following steps are used when the device joins the network.

(1) Integrated the Device into the Network.

- **a)** To agree the transmission protocol and speed.
- **b)** To configure node addresses, routing information and another resources.

(2) To discovery of the Services and Resources Offer by the Devices.

- **a)** To discover the services and different resources shared in the network.
- **b)** We have a list of services and resources available in the network they can update.

(3)To access the services offered by the Devices.

- **a)** To manage the automatic integration tasks and the use, for example, agent service.
- **b)** Manage access security to the services.
- **c)** To manage join and leave the nodes in the network.

(4) The collaborative task.

- **a)** Only within the intranet, among the various members.
- **b)** On the internet, with the other communication.

2.2 Network Model:

The first node is responsible for set up the spontaneous network. However each node configure their own data i.e. IP port and user data. Devices must be aware of all different tasks needed to communicate with each other and the configuration of logical and physical parameters when they join network. Users save their resources to the system. The connection can be shared and that device will provide the access to the WWW, if one of the users of the spontaneous network have the Internet connection. Internet access in the spontaneous network could be more than one and each one of them can share different services they are available. Components contains the private key. when a user join the spontaneous network that are following ways:

- **(1)** Node identifies.
- **(2)** Identification between the nodes.
- **(3)** Address assignment of the nodes.
- **(4)** To join services in the network.

2.3 Security in spontaneous network:

Portable nodes that need to communicate to reduce time slot for the creation of spontaneous ad hoc networks. The problems of ad hoc network are similar to these networks, but they increased because they are temporal networks form in a given that moment by a group of nodes that often users don't know each other. However, they can work together for the proper process of the network. Safe communication must be guarantee with the help of cryptographic techniques. However, many of the outlined protocols assume that every node know the session key, When we talk about the use of cryptography of private key as well as the cryptography of public key. Methods to establish a secure and authentic communication channel is provided by these networks, assuming that the participants know the node which they are speaking with them and share the data. A fundamental topic in the security of the spontaneous networks creation, when the nodes do not know each other and also the phase of connection establishes and initial exchange of keys. Security requirements in spontaneous networks and traditional networks are same: privacy, integrity, Verification, no repudiation, and availability, confidentiality. Both data as well as routing information must be safe. The structures of ad hoc networks make these necessities much more difficult: dynamic topology, limited bandwidth, different capacity links and high error rates, energy and processing capacity Limitations, no central server, and often no prior information in the nodes to build the network. These limitations have to be covered by organization mechanisms and by the support among the nodes to maintain service quality, security, and almost inventions and access to the Services and share data. Like human relationships in the society, this Behavior is also similar to them. Everyone must cooperate to preserve a secure world, to improve our quality of life, and have updated news. We know that the data should be correct when they come from a person that we trust. In this society the trust is very important. Our goal to develop technique in order to enable the creation of small-medium-scale ad hoc networks based on the spontaneity of both. On the grounds of physical proximity, wireless connectivity is based; it reflects the ways of the human beings interact. People who are near each other can link, share things with the each other, and ask people to relay information to other users. That is all done with an appropriate Level of security. To get an appropriate level of security we establish numerous protection mechanisms as follows.

- **i.** Identity of the Nodes
- **ii.** Prevention of Proud Behaviour
- **iii.** The Security in Routing Protocols against Manipulations.

Also by providing the intrusion detection scheme that provides more security of joining the new node in the network.

3. Conclusion:

In this paper provide complete self-configured secure protocol which is described gives more trusted way to spontaneous ad hoc network with every node maintain the network, improves the services offered, and provide information to other network node for the Formation Spontaneous ad hoc networks. The protocol allows secure communication between end users includes the security schemes, with the help of intrusion detection provide more security and share the data.

4. 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. CSU, S. Seta, 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]. 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.

[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),. 2004.

[8]. 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.

[9]. 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.

[10]. L. Herrero and R. Lacuesta, “A Security Architecture Proposal for Spontaneous Networks,” Proc. Int’l Conf. Advances in the Internet Processing System and Interdisciplinary Research, Oct. 2003.

[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.M. Feeney, B. Ahlgren, and A. Westerlund, “SpontaneousNetworking:An Application-Oriented Approach to Ad-hocNetworking,” IEEE Comm. Magazine, vol. 39, no. 6, pp. 176-181, June 2001

[13]. R. Lacuesta, J. Lloret, M. Garcia, and L. Pen˜ alver, “A Spontaneous Ad-Hoc Network to Share WWW Access,” EURASIP J. Wireless Comm. and Networking, vol. 2010, article 18, 2010.