International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 7 Issue 1 –MARCH 2014.

SECURING SPONTANEOUS WIRELESS ADHOC NETWORK CREATION WITH SECRET KEY TECHNIQUES

Mr.P.Siva sankar (Asst.Professor)
Dr .Pauls Engineering College

Ms.K.Karpagalakshmi (PG Scholar)
Dr .Pauls Engineering College

Abstract- A secure protocol for spontaneous wireless ad hoc networks which uses a hybrid symmetric/ asymmetric 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. Trust is based on the first visual contact between users. To built a complete self-configured secure protocol that is able to create the network and share secure services without any infrastructure. The network allows sharing resources and offering new services among users in a secure environment. The protocol includes all functions needed to operate without any external support. The designed and developed it in devices with limited resources. In the existing system, there is no proper security measures were implemented in Wireless Ad-hoc Networks while joining new nodes and exchanging data. In the proposed system, if a new node want to with the existing node, the new node will send the request to the existing node. Based on the request, the existing node will send its public key to the new node. After that the new node and existing node will share their public and private key components to authenticate each other. For security purpose the data will be encrypted during transmission. The Certificate Authority is used to authorize the node when it wants joins another node. Secret key is generated, which is used to share the data and it will be changed at a particular period of time. In the modification process, the secret key is also changed when the node joins a network and leaves a network. So that we can increase the level of security. The goal is to design of a protocol that allows the creation and management of a spontaneous wireless ad hoc network. It is complete self configured secure protocol that is able to create network and share secure services without any external infrastructure. The network allows sharing resources and offering new services among users in secure environment. Using cryptographic secret key technique to improve a level of security.

I. INTRODUCTION

A wireless ad hoc network is a decentralized type of wireless network. The network is ad hoc because it does not rely on a preexisting infrastructure, such as routers in wired networks or access points in managed infrastructure wireless networks. Instead, each node participates in routing by forwarding data for other nodes, so the determination of which nodes forward data is made dynamically on the basis of network connectivity. In addition to the classic routing, ad hoc networks can use flooding for forwarding the data.

The exponential growth in the development and acceptance of mobile communications in recent years is especially observed in the fields of wireless local area networks, mobile systems, and ubiquitous computing. This growth is mainly due to the mobility offered to users, providing access to information anywhere, user friendliness, and easy deployment. Furthermore, the scalability and flexibility of mobile communications increase users' productivity and efficiency.

Spontaneous ad hoc networks are formed by a set of mobile terminals placed in a close location that communicate with each other, sharing resources, services or computing time during a limited period of time and in a limited space, following human interaction pattern. People are attached to a group of people for a while, and then leave. Network management should be transparent to the user. A spontaneous network is a special case of ad hoc networks. They usually have little or no dependence on a centralized administration.

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 failure of one of the devices or services does not compromise the viability of the community. Any resources being used by the community which malfunction are 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 resources 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 techniques 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 established. There are many application areas for ad hoc spontaneous networks: industrial is communication between sensors, robots, and digital networks, business is meeting, stock control, etc., military is hard and hostile environments, and teaching. The range 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.

The design and simulation of a model that lets optimal spontaneous network access using a caching mechanism. We present the procedure of the nodes involved in the system, the security algorithms implemented, and the designed messages. Moreover, we included the analytical proposal and its comparative with the most similar protocols in the literature. The validation of the protocol is carried out through several simulations and comparisons with regular architectures. The proposal has been developed with the main objective of improving the communication and integration between different study centers of low-resource communities.

II. SYSTEM DESIGN

In MANETS components are classified into
1. Network Setup Module , 2.Trusted User and node creation Module , 3.New node Joining Module, 4. New network creation module, 5. Data transfer module
1) Network setup model:
The user can register and login with the owner permission whether to join new node and or an existing node or to create a network.The owner provides session key based on the requirements of the trusted user.
2) Trusted User and node creation Module:
The data is shared between two trusted users by session key generation for their respective data's and encrypting their files. The user can only access the data file with the encrypted key if the user has the privilege to access the file. Validation of integrity and authentication is done automatically in each node and this forms a Spontaneous Wireless Ad Hoc node creation between trusted authorities (users).
3) New node Joining Module:
By using Network based Intrusion Detection System (NIDS),the new node is created and they are joined to new nodes by respective procedures given by owner.
The joining module is done with 3 phases:
(i) Joining Procedure
(ii) Services Discovery
(iii) Establishing Trusted Chain and Changing Trust Level
4) New network creation module:
Create a new network for the trusted users.The first node in the network will be responsible for setting the global settings of the spontaneous network.The second node first configures its user data and network security.Our protocol relies on a sub layer protocol **eg.**Bluetooth.After encountering the device, the authentication request is sent to another user.If authentication is accepted, it asks for data exchange. If failed the device wont exchange data.
5) Data transfer module:
A node receives a data packet that is ciphered by a public key.When the server process received the packet, it is in charge of deciphering it with the private key of the user.

III. SYSTEM ARCHITECHTURE

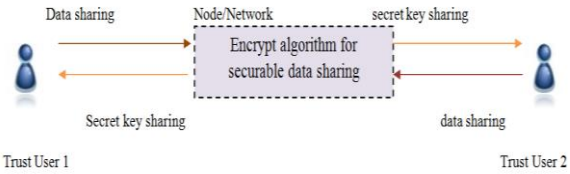

Fig 3.1. Architecture diagram for Secure Protocol for Spontaneous Wireless Ad Hoc Networks Creation

This diagram shows secret key and data sharing between a two trusted user. If a new node want to with the existing node, the new node will send the request to the existing node. Based on the request, the existing node will send its public key to the new node. After that the new node and existing node will share their public and private key components to authenticate each other. For security purpose the data will be encrypted during transmission.

This step enables devices to communicate, including the automatic configuration of logical and physical parameters. The system is based on the use of an IDentity Card (IDC) and a certificate.

The IDC contains public and private components. The public component contains a Logical Identity (LID), which is unique for each user and allows nodes to identify it. It may include information such as name, photograph or other type of user identification. This idea has been used in other systems such as in vehicular ad hoc networks . It also contains the user's public key (Ki), the creation and expiration dates, an IP proposed by the user, and the user signature. The user signature is generated using the Secure Hash Algorithm (SHA-1) on the previous data to obtain the data summary. Then, the data summary is signed with the user's private key. The private

component contains the private key (ki). The user introduces its personal data (LID) the first time he/she uses the system because the security information is generated then. Security data are stored persistently in the device for future use. Certificate Cij of the user i consists of a validated IDC, signed by a user j that gives its validity. To obtain IDC signature of user i, the summary function obtained by SHA- 1 is signed with j's private key. No central certification authority is used to validate IDC. Validation of integrity and authentication is done automatically in each node. The certification authority for a node could be any of the trusted nodes.This system enables us to build a distributed certification authority between trusted nodes. When node A wants to communicate with another node B and it does not have the certificate for B, it requests it from its trusted nodes. After obtaining this certificate the system will validate the data; if correct then it will sign this node as a valid node. All nodes can be both clients and servers, can request or serve requests for information or authentication from other nodes.

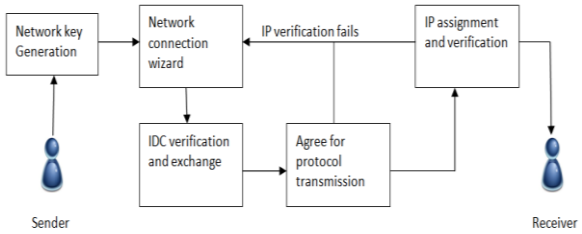

Fig 3.2. Architecture diagram for New Node

The first node creates the spontaneous network and generates a random session key, which will be exchanged with new nodes after the authentication phase. Fig. 3.2. shows phases of a node joining the network: node authentication and authorization, agreement on session key, transmission protocol and speed, and IP address and routing. When node B wants to join an existing network, it must choose a node within communication range to authenticate with (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. 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 data, services, and other nodes certificates by a route involving other nodes in network.

IV EXISTING SYSTEM

The existing system objective is the integration of services and devices in the same environment, enabling the user to have instant service without any external infrastructure. Because these networks are implemented in devices such as laptops, PDAs or mobile phones, with limited capacities, they must use a lightweight protocol, and new methods to control, manage, and integrate them. Methods based on imitating the behavior of human relations facilitate secure integration of services in spontaneous networks. Furthermore, cooperation among the nodes and quality of service for all shared network services should be provided.

Drawbacks in existing system

All nodes may not be able to execute routing and/or security protocols. Energy constraints, node variability, error rate, and bandwidth limitations mandate the design and use of adaptive routing and security mechanisms, for any type of devices and scenarios.

Dynamic networks with flexible memberships, group signatures, and distributed signatures are difficult to manage.To achieve a reliable communication and node authorization in mobile ad hoc networks, key exchange mechanisms for node authorization and user authentication are needed security methods such as pre-distribution key algorithms, symmetric and asymmetric algorithms, intermediate node-based methods, and hybrid methods. But these methods are not enough for spontaneous networks because they need an initial configuration or external authorities

V PROPOSED SYSTEM

The network and protocol proposed in this paper can establish a secure self-configured environment for data distribution and resources and services sharing among users. Security is established based on the service required by the users, by building a trust network to obtain a distributed certification authority. A user is able to join the network because he/she knows someone that belongs to it. Thus, the certification authority is distributed between the users that trust the new user. The network management is also distributed, which allows the network to have a

distributed name service. We apply asymmetric cryptography, where each device has a public-private key pair for device identification and symmetric cryptography to exchange session keys between nodes. There are no anonymous users, because confidentiality and validity are based on user identification.

Advantages of proposed system

We presented the basis to setup a secure spontaneous network.To solve mentioned security issues, we used an authentication phase and a trust phase.We presented a mechanism to allow nodes to check the authenticity of their IP addresses while not generating duplicated IP addresses. The mechanism helps nodes to authenticate by using their IP addresses. We have used this mechanism in the secure protocol presented in this paper, but it can be replaced by any other IP address assignment mechanism.

It presents two secure and energy-saving spontaneous ad hoc protocols for wireless mesh client networks where two different security levels (weak and strong) are taken into account in the path when information is transmitted between users.These public keys are used to calculate a shared secret session key for encrypted communication. a secure spontaneous network protocol based on user trust that provides node authenticity, integrity checking, and privacy.

VI PROTOCOL OPERATION

In order to design the diagrams of the protocol, we have used the Unified Modeling Language (UML). The UML is a visual specification standardized language that is built to model object oriented systems. We use keys, activities, and use cases (diagrams offered by the standard) to define the processes, the structure of the classes in the system, and the behavior of objects or operations.

use case diagram:

A use case diagram in the Unified Modeling Language (UML) is a type of behavioral diagram defined by and created from a Use-case analysis. Its purpose is to present a graphical overview of the functionality provided by a system in terms of actors, their goals (represented as use cases), and any dependencies between those use cases. The main purpose of a use case diagram is to show what system functions are performed for which actor. Roles of the actors in the system can be depicted.

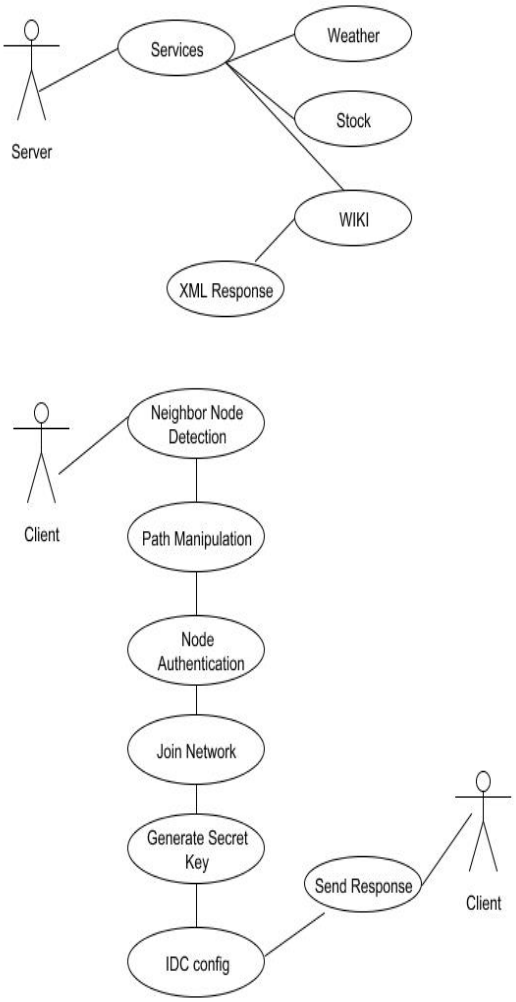

Fig 5.1 Usecase diagram

sequence diagram:

A sequence diagram in Unified Modeling Language (UML) is a kind of interaction diagram that shows how processes operate with one another and in what order. It is a construct of a Message Sequence Chart. Sequence diagrams are sometimes called event diagrams, event scenarios, and timing diagrams.

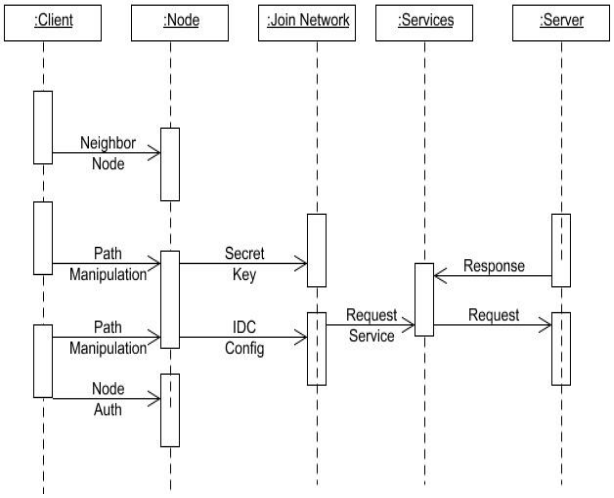

Fig 5.2 Sequence diagarm

VII CONCLUSION

The design of a protocol that allows the creation and management of a spontaneous wireless ad hoc network. It is based on a social network imitating the behavior of human relationships. Thus, each user will work to maintain the network, improve the services offered, and provide information to other network users. We have provided some procedures for self-configuration: a unique IP address is assigned to each device, the DNS can be managed efficiently and the services can be discovered automatically. We have also created a user-friendly application that has minimal interaction with the user. A user without advanced technical knowledge can set up and participate in a spontaneous network. The security schemes included in the protocol allow secure communication between end users (bearing in mind the resource, processing, and energy limitations of ad hoc devices). We have performed several tests to validate the protocol operation. They showed us the benefits of using this self-configuring ad hoc spontaneous network. The response times obtained are suitable for use in real environments, even when devices have limited resources. Storage and volatile memory needs are quite low and the protocol can be used in regular resource-constrained devices (cell phones, PDAs...). We intend to add some new features to the user application (such as sharing other types of resources, etc.) and to the protocol, such as an intrusion detection mechanism and a distributed Domain Name Service by using the LID and IP of the nodes. Now, we are working on adding other types of nodes that are able to share their services in the spontaneous network. The new nodes will not depend on a user, but on an entity such as a shop, a restaurant, or other types of services.

VIII FUTURE ENHANCEMENT

We intend to add some new features to the user application (such as sharing other types of resources, etc.) and to the protocol, such as an intrusion detection mechanism and a distributed Domain Name Service by using the LID and IP of the nodes. Now, we are working on adding other types of nodes that are able to share their services in the spontaneous network.

The designing of complete self configured secure protocol that is able to create network and share secure services without any external infrastructure. Using cryptographic secret key technique to improve a level of security.

IX REFERENCES

[1] 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.

[2] J. Lloret, L. Shu, R. Lacuesta, and M. Chen, "User-Oriented and Service-Oriented Spontaneous Ad Hoc and Sensor Wireless Networks," Ad Hoc and Sensor Wireless Networks, vol. 14, nos. 1/ 2, pp. 1-8, 2012.

[3] S. Preuß and C.H. Cap, "Overview of Spontaneous Networking - Evolving Concepts and Technologies," Rostocker Informatik- Berichte, vol. 24, pp. 113-123, 2000.

[4] 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.

[5] Y. Xiao, V.K. Rayi, B. Sun, X. Du, F. Hu, and M. Galloway, "A Survey of Key Management Schemes in Wireless Sensor Networks," Computer Comm., vol. 30, nos. 11/12, pp. 2314-2341, Sept. 20

Karpagalakshmi.K received B.Tech (Information Technology)degree from Anna University in 2011.Currently pursuing M.E (Computer and Communication) in Dr.Pauls Engineering College. Presented a paper in National Conference entitled as "Securing Spontaneous Wireless Adhoc Network Creation with Secret Key Techniques". Her area of interest includes wireless Networks and Web Technology.

Sivasankar .P was born in karaikal, Indiain 1982. He received his Bachelor of Technology degree in Computer science Engineering, from Pondicherry University, Pondicherry and Master of Engineering degree in Wireless Technology from Anna University, Madurai, India. Currently he is working as assistant professor in Dr. Pauls Engineering College, Villupuram and affiliated to Anna UniversityChennai, Tamil Nadu, India. His area of interest includes wireless communication and wireless networks.