Performance Based Secure Protocol Methodology for Spontaneous Wireless Mobile Adhoc Networks

Ashish A. Patil , Deepika M. Shinde, Chaitali C. Shinde, Rohit D Sambre, Prof. H. D. Sonawane

***Abstract*— This proposed system presents 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. Our proposal is 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. We have designed and developed it in devices with limited resources. Network creation stages are detailed and the communication, protocol messages, and network management are explained. Our proposal has been implemented in order to test the protocol procedure and performance. 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.**

***Index Terms*— Network, Protocol, Node, IP Address, Session key, Encryption.**

I. INTRODUCTION

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. Spontaneous networks can be wired or wireless. We consider only wireless spontaneous networks in this paper. Their objective is the integration of services and devices in the same environment, enabling the user to have instant service without any external infra-structure. 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. Configuration services in spontaneous networks depend significantly on network size, the nature of the participating nodes and running applications. Spontaneous networks imitate human relations while having adaptability to new conditions and fault tolerance (the failure of a device or service should not damage the functionality). Methods based on imitating the behavior of human relations facilitate secure integration of services in spontaneous networks. Further-more, cooperation among the nodes and quality of service for all shared network services should be provided.

Spontaneous ad hoc networks require well defined, efficient and user-friendly security mechanisms. Tasks to be performed include: user identification, their authorization, address assignment, name service, operation, and safety. Generally, wireless networks with infrastructure use Certificate Authority (CA) servers to manage node authentication and trust. Although these systems have been used in wireless ad hoc and sensor networks , they are not practical because a CA node has to be online (or is an external node) all the time. Moreover, CA node must have higher computing capacity. Security should be based on the required confidentiality, node cooperation, anonymity, and privacy. Exchanging photos between friends requires less security than ex- changing confidential documents between enterprise man- agers. Moreover, 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.

The related literature shows several security methods such as redistribution 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 (i.e., network configuration) or external authorities (for example, central certification authorities).

None of the existing papers propose a secure spontaneous network protocol based on user trust that provides node authenticity, integrity checking, and privacy. The network and protocol proposed in this paper can establish

Manuscript received January 03, 2015.

Ashish A. Patil , Department of Computer Engineering, BVCOE & RI, Nashik (India).

Deepika M. Shinde, Department of Computer Engineering, BVCOE & RI, Nashik (India).

Chaitali C. Shinde, Department of Computer Engineering, BVCOE & RI, Nashik (India).

Rohit D Sambre, Department of Computer Engineering, BVCOE & RI, Nashik (India).

Prof. H. D. Sonawane, Department of Computer Engineering, BVCOE & RI, Nashik (India).

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.

Preliminary versions of this paper appeared in 2003, we presented the basis to setup a secure spontaneous network. To solve mentioned security issues, we used an authentication phase and a trust phase. Moreover, 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.

II. OBJECTIVES

Advances in wireless local-area network technology typically based on IEEE 802.11 and the growing interest in public safety communications have created new demands for reliable transmission of real-time multimedia information over distributed mobile ad hoc networks (MANET). The objective of this project is to test and evaluate the performance of MANET for safety communications and tactical operations. In particular, by providing diversity cooperative transmission can indeed increase throughput as well as transmission coverage. In this study we will specifically concentrate on the synchronization aspects of cooperative transmission, which is one of the major issues in its application to multi-hop transmission in wireless ad-hoc network environments. The main focus will be to address quality of service issues and network reliability for transmission of real-time information. Specifically, we are pursuing the following tasks:

1. Space-time diversity routing for cooperative transmission
2. Directional routing based on smart antenna

In mobile multi-hop network communications, multipath fading and interference can severely degrade the throughput, particularly for real-time transmission of multimedia information. This project is mainly concerned with enhancing the multi hop link performance under fast fading conditions. The main goal is to develop a tested to evaluate network performance for data, voice and video services.

III. PROBLEM STATEMENT

Classification of mobile apps is considered as a quite difficult task. This is because for having a proper or effective classification we need to have detailed information about the app. This is challenging task as very limited contextual information about the app is available. To be specific contextual information obtained from the apps name is very limited, as the words used for app name are very short and sparse. Hence there is an immediate need to provide an effective classification of the mobile apps by using the enriched information about the apps.

To achieve this goal, we will be exploiting not only the web knowledge but also the real world contextual features about the apps along with their word labels. This will automatically improve the contextual information of the apps, resulting into improved performance of the classification. Here the web knowledge is extracted from the general search engine like Google or from the app store, while the real world features will be extracted from the mobile usage record of the user.

IV. 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

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.

A. User 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

- In this module, the trusted user gets login by admin permission.

- 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.

B. Administrator Module:

1. 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

2. New network creation module

- In this module, we 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 e.g. Bluetooth, Wi-Fi

3. 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.

VI. SYSTEM DEVELOPMENT

Step 1: Joining Procedure

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.

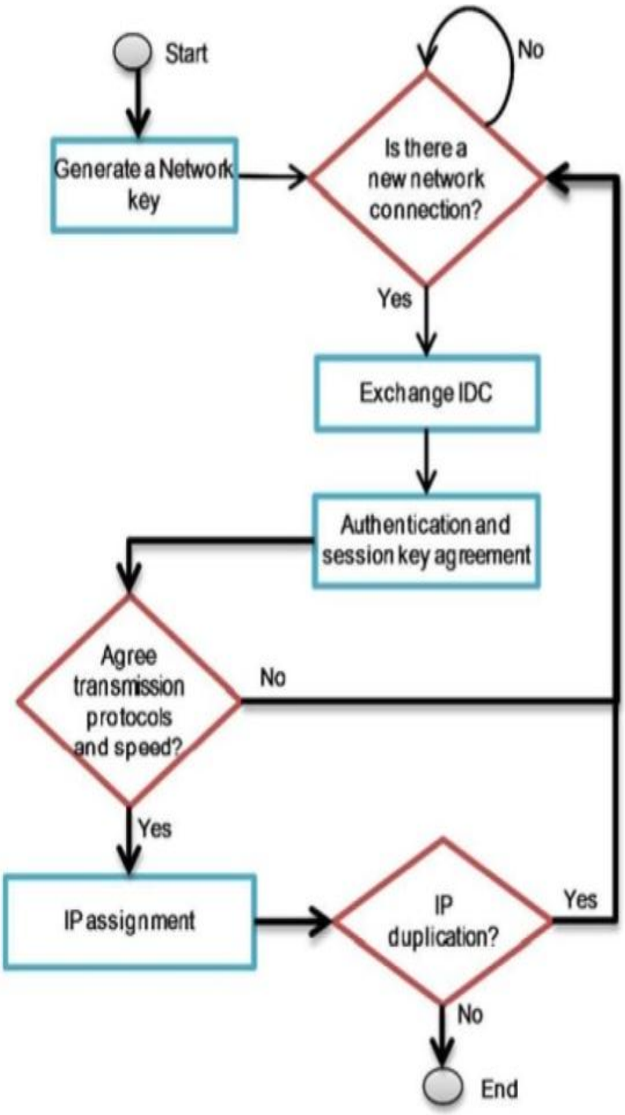
Start
Generate a Network key
Is there a new network connection?
No
Yes
Exchange IDC
Authentication and session key agreement
Agree transmission protocols and speed?
No
Yes
IP assignment
IP duplication?
Yes
No
End

Fig. 1. Algorithm for joining a 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. 1 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. Symmetric key is used as a session key to cipher the confidential messages between trust nodes. It has less energy requirements than the asymmetric key. We have used the Advanced Encryption Standard (AES) algorithm for the symmetric encryption scheme. It offers high security because its design structure removes sub key symmetry. Moreover, execution times and energy consumption in cryptography processes are adequate for low-power devices. The asymmetric key encryption scheme is used for distribution of the session key and for the user authentication process. We used two types of asymmetric encryption schemes: Elliptic Curve Cryptosystem (ECC), because of its high performance, and the Rivets, Shamir & Adelman cryptographic algorithm (RSA). After the mutual authentication, A will encrypt the session key with B's public key and will send it to B. Then, they will agree the transmission protocols and the wireless connection speed.

Finally, B will configure IP address and routing information. Secure routing protocol is borrowed from. B generates an IP address which has a fixed part in the first two bytes and the rest is formed by a random number which depends on the user's data. Then, B will send the data to process the routing information to A. A will check whether the IP is duplicated in the network. When B sends data to other network nodes, e.g., node C, these data will be validated by C (using hashing and authentication methods). Afterwards, C will establish the trust level with B, by looking physically. If no trust level is established, it will be done afterwards by using trusted chains.

Step 2: Services Discovery

Stemming is the term used in linguistic morphology and information retrieval to describe the process for reducing in selected (or sometimes derived) words to their word stem, base or root form-generally a written word form. The stem needs not to be identical to the morphological root of the word; it is usually sufficient that related words map to the same stem, even if this stem is not in itself a valid root. Many search engines treat words with the same stem as synonyms as a kind of query expansion. Preprocessing steps to save both space and time requirements by using improved Stemming Algorithm. Stemming algorithms are used to transform the words in texts into their grammatical root form. Several algorithms exist with different techniques. The most widely used stemming algorithm is Porter stemming algorithm.

Step 3: Establishing Trusted Chain and Changing

There are only two trust levels in the system. Node An either trusts or does not trust another node B. The software application installed in the device asks B to trust A when it receives the validated IDC from B. Trust relationship can be asymmetric. If node A did not establish trust level with node B directly, it can be established through trusted chains, e.g., if A trusts C and C trusts B, then A may trust B. 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.

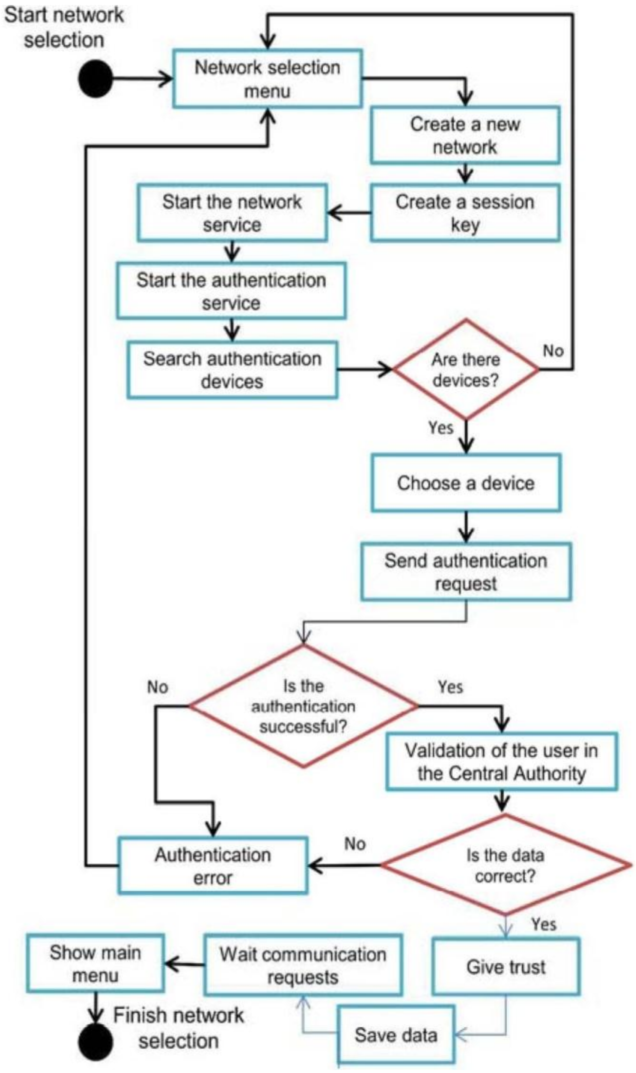

Fig 2. New network creation procedure

VII. PROTOCOL OPERATION

The authenticated node can perform the following tasks:

- Display the nodes.
- Modify the trust of the nodes.
- Update the information: It allows a node to learn about other nodes in the network and also to send its data to the network. This update could be for only one user or for all users in the network through a controlled diffusion process.
- Other nodes certificate request: A node could be requested from other node, from all trusted nodes or from all known nodes. In case of all known nodes, the node that replies to the request will always sign the data. The data will be considered validated if a trusted node has signed them.
- Process an authentication request: The node authenticates a requesting node by validating the received information, user authentication, and verifying the no duplication of the LID data and the proposed IP.
- Reply to an information request: the requested information will be sent directly to the requesting node or routed if the node is not on the communication range.

- Forward an information request: The request will be forwarded if it is a broadcast message.

- Send data to one node: It can be sent symmetrically or asymmetrically encrypted, or unencrypted.

- Send data to all nodes: This process is doing by a flooding system. Each node retransmits the data only the first it receives the data. It can be sent symmetrically encrypted or unencrypted.

- Modify Data: User data can be modified and the password changed.

- Leave the network.

VIII. CONCLUSION

In This Project, we show 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.

ACKNOWLEDGMENT

It is my pleasure to express my knowledge to my respected sir Prof. H. D. Sonawane, Computer Engineering Department, BVCOE&RI, Nashik for his valuable guidance, inspiration and continues support. This paper could not be success without protocol study done which help to understand the necessity for this paper.

REFERENCES

[1] 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.

[2] 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. 2007.

[3] V. Kumar and M.L. Das, “Securing Wireless Sensor Networks with Public Key Techniques,” Ad Hoc and Sensor Wireless Networks, vol. 5, nos. 3/4, pp. 189-201, 2008.

[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] A. Noack and S. Spitz, “Dynamic Threshold Cryptosystem without Group Manager,” Network Protocols and Algorithms, vol. 1, no. 1, Oct. 2009.

[6] J. Yan, J. Ma, F. Li, and S.J. Moon, “Key Pre-distribution Scheme with Node Revocation for Wireless Sensor Networks,” Ad Hoc and Sensor Wireless Networks, vol. 10, nos. 2/3, pp. 235-251, 2010.

[7] M. Mukesh and K.R. Rishi, “Security Aspects in Mobile Ad Hoc Network (MANETs): Technical Review,” IJCA, vol. 12, no. 2, pp. 37-43, Dec. 2010