International Journal of Security and Its Applications
Vol. 10, No. 6 (2016) pp.37-46
http://dx.doi.org/10.14257/ijsia.2016.10.6.05

User Revocation Mechanism for Service Oriented Wireless Adhoc Networks

Reddi Prasadu[1], M. Jeevan Babu[1], Sk. Mohammed Gouse[1],
Debnath Bhattacharyya[2] and Tai-hoon Kim[3]

[1] *Department of Computer Science and Engineering, KL University, Vaddeswaram, AP, 522502, India*
[2] *Department of Computer Science and Engineering, Vignan's Institute of Information Technology, Visakhapatnam-530049, India*
[3] *Department of Convergence Security, Sungshin Women's University, 249-1, Dongseon-dong 3-ga, Seoul, 136-742, Korea*
(Corresponding Author)
{reddiprasad0112, jeevan.projects, mohammadgousesk11}@gmail.com[1], debnathb@gmail.com[2], taihoonn@daum.net[3]

Abstract

Adhoc network is basically infrastructure less in nature and it is vulnerable to attacks. In such a network it is necessary to create the security autonomously without the involvement of centralized architecture. Address allocation, name resolution, services rendering, authentication and access control policies represent some of the functionalities that are supported by the Adhoc Networks. To solve the above issue, a novel security protocol is proposed for the Passionate network formation. Initial network formation done based on trust. For each newly added user authorization is performed using certificate generation. Authentication is carried out using certificate verification mechanism. Session key is used by all the nodes in the network, for the defended communication. Symmetric key encryption is used for data encryption. Asymmetric cryptography is used for session key encryption and signature generation. Session key updating is carried out based on expiration time. To revoke the attacker from participating in the network, User revocation mechanism is contributed to the proposed security protocol. Security is enhanced with revocation capabilities.

Keywords*: Centralized architecture, Symmetric and asymmetric cryptographies, Defended protocol*

1. Introduction

Adhoc network is created for a group of people who come together for some collaborative activity. This helps in establishing basic services and security infrastructure. For this purpose we can use the human interactions associated with the activity. Ad hoc networking presents two distinct challenges:

1. The network must operate independent of an access point infrastructure.

2. The network must operate independent of a pre-established or centralized network management infrastructure.

Since the network population and topology are not known in advance nor can be preconfigured, so services in ad hoc environment cannot be centralized. Nodes may need to cooperate to provide functionality such as group communication replicated object storage, caching and remote object invocation. In fixed network encryption keys, certificates, authorization information stored in trusted repositories both local and global

ISSN: 1738-9976 IJSIA

are the key issues on which security depend. But in ad hoc environment, it is necessary to support key distribution for encrypting traffic in the wireless media and authentication of users and devices in the absence of a global identity database. To obtain useful results, the ability to route traffic from one node to another is not sufficient instead the problem of administration in ad hoc networks has received little attention. Applications such as interactive presentation collaborative editing, shared white boards and games are ideal candidates for operations in such as environment. Intentional interactions among users who have chosen to collaborate for some purpose are reflected by network. Our goal is to empower users to create computer networks with same ease, flexibility and spontaneity as the human interactions they are intended to facilitate.

Passionate networking environment proposed five key challenges where each reflects some way in which a Passionate network differs from other well known infrastructure or mobile computing environments; and are given below:

Network boundaries are poorly defined: "Coming up on a network" simply means enabling the network interface and connecting to and possibly authenticating with the networking infrastructure in conventional wired or wireless network. In an infrastructure less network, there is no natural equivalent.

There is no planned network: Conventional networks are not built on an ad hoc basis; Logical and administrative boundaries suggest where services should be hosted and replicated.

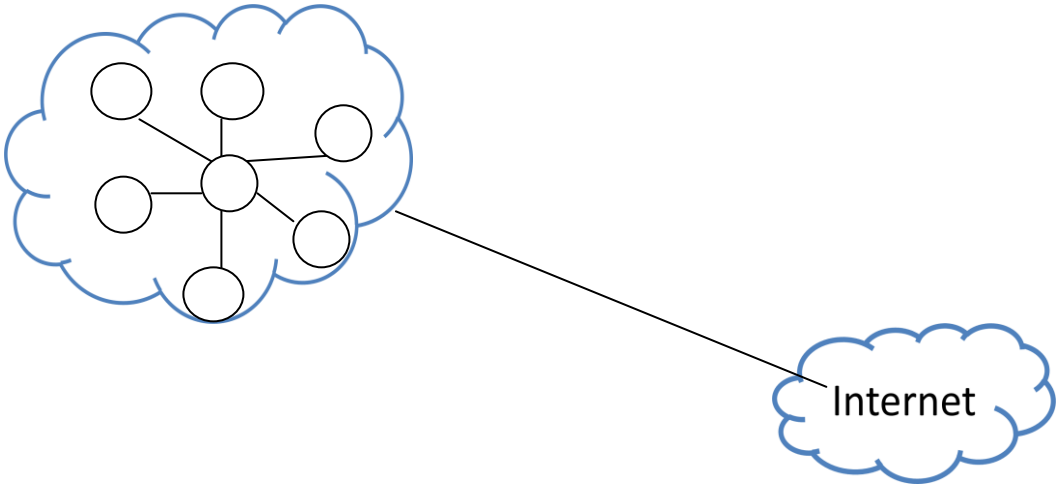

Figure 1. Sample Adhoc Network

Pre configuration of hosts doesn't exist: Since these Passionate networks are created at anytime and anywhere: Information such as Network Access Identifier's (NAI) or user principals of the participants, the host names and addresses of the nodes, available services and the nodes where they are hosted cannot be predetermined. Therefore, nodes and services cannot be preconfigured with this information.

There are no central servers: Within an ad hoc network, there is no well defined primary version of an object to which all modifications must eventually be committed. In fact, users can be disconnected from their home infrastructure and operating in a Passionate networking environment at the same time.

There are no experts: Users are notoriously bad at configuration, especially in an environment that poses complex security issues. Operation must be intuitive to non technical users. And hence it is necessary to minimize the inexpert users' exposure to the administrative infrastructure and make necessary activities as intuitive as possible.

2. Related Work

A defended Passionate ad-hoc network is presented, which is based on direct peer-to-peer interaction, to grant a quick, easy, and defended access to the users to surf the Web. The literature shows the description of our proposal, the procedure of the nodes involved in the system, the security algorithms implemented, and the designed messages. This literature has taken into account the security and its performance. Although some people have defined and described the main features of Passionate ad-hoc networks, nobody has published any design and simulation until today. Passionate networking will enable a more natural form of wireless computing when people physically meet in the real world. [1]

The design and implementation of public-key-(PK)-based protocols that allow authentication and key agreement between a sensor network and a third party as well as between two sensor networks. Our work is novel in that PK technology was commonly believed to be too inefficient for use on low-power devices. The TinyPK system demonstrates that a public-key based protocol is feasible for an extremely lightweight sensor network. Incorporating the use of TinySec or any other symmetric encryption service for mote networks, TinyPK provides the functionality needed for a mote and a third-party to mutually authenticate to each other and to communicate defendedly. As part of solution, the efficiency of public operations are exploited in the RSA cryptosystem and design protocols that place the computationally expensive operations on the parties external to the sensor network, when possible. [2]

In this literature, the energy cost of authentication and key exchange based on public-key cryptography on an 8-bit microcontroller platform has been quantified. A comparison of two public-key algorithms, RSA and Elliptic Curve Cryptography (ECC), has been presented and mutual authentication and key exchange between two untrusted parties are considered such as two nodes in a wireless sensor network. Low-power microcontroller indicates that public-key cryptography is very viable on 8-bit energy constrained platforms even if implemented in software. It is found that ECC to have a significant advantage over RSA as it reduces computation time and also the amount of data transmitted and stored. [3]

Passionate networking is a means for simple integration of devices and services into networks. It seems to be one way to achieve more flexibility, more mobility, a better usability and less administration effort. This paper provides a definition of Passionate networking and lists mandatory and optional features. It takes a closer look at the evolving technologies Jini (Java intelligent network infrastructure), JetSend, Inferno/Limbo, HAVi (Home Audio Video interoperability), and UPnP (Universal Plug and Play). Passionate is not used in the meaning of not constrained or voluntary but in the meaning of automatic or self-regulated. Therefore, Passionate networking is referenced here as the integration of services and devices into network environments with the objective of an instantaneous service availability without any manual intervention. [4]

Most ad hoc networks do not implement any network access control, leaving these networks vulnerable to resource consumption attacks where a malicious node injects packets into the network with the goal of depleting the resources of the nodes relaying the packets. To thwart or prevent such attacks, it is necessary to employ authentication mechanisms to ensure that only authorized nodes can inject traffic into the network. A hop-by-hop authentication protocol called LHAP has been proposed for ad hoc networks. LHAP resides in between the network layer and the data link layer, thus providing a layer of protection that can prevent or thwart many attacks from happening, including outsider attacks and insider impersonation attacks. [5]

A set of mobile terminals placed close to each other forms a Passionate ad hoc network on sharing resources, computing time in a limited space by following human interaction pattern. Passionate Networks are special case of ad hoc networks where the

network management is transparent to user. Our proposal is to provide a defended network without infrastructure and reject the false (untrusted/malicious) users. Security is based on the confidentiality, privacy, node cooperation and anonymity. And to achieve reliable communication and node authorization: user authentication and key exchange mechanisms for node authorization are needed in mobile ad hoc networks.

3. Passionate Network Formation

3.1. Overview of a Network

The network users1 (also sometimes referred as node if required) and services may vary with time because a user can join and leave the network at wish. The network formation mainly consists of three phases in order to provide defended transfer of data from one user to other.

Joining a User: The system is based on IDC (IDentity Card) and certificate. IDC contains both public and private components. The public component contains Logical Identity (LID), which is unique to each user and allow others to identify it. If there is no existing network then a user should initiate him/her in order to create it. User is sometimes referred as node in the paper as required.

Services Discovery: A user can know the services by asking the other users about the services available with them. Since we do not maintain a central server here the services can be rendered using Web Services Description Language (WSDL). Most of the parameters of services aren't transparent instead they need manual configuration.

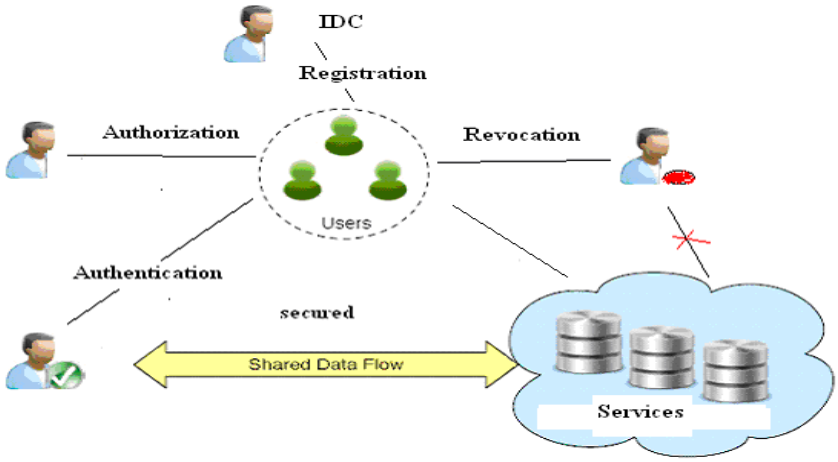

Figure 2. Architecture of Passionate Adhoc Network

Trust Establishment: Trust relationship can be asymmetric and can change over time depending on node's behavior. There are only two Trust levels in the system as follows:

1. *Zero level:* Since there is no authentication process done by the devices there is no trust and the trust level is put down.

2. *First level:* Here the authentication process is performed and the devices trust each other.

We also have two validity levels as follows:

1. *Zero level:* The key is not valid because it has neither been obtained in the validation process of nor a trust device.

2. *First level:* The key is valid because it has obtained the pre-authentication phase through a trusted device.

3.2. Network Formation

The network is created using the information provided by users, hence, each node is identified by an IP address and the servers are shared using TCP connections. Each node learns the identity card of other known nodes, public key and LID, after the authentication process. This information is updated and completed throughout the network nodes. The first node is responsible for setting the global settings of Passionate network and changes to standby mode in order to service the requests. Each node needs to configure its own data by them. The process is clearly explained through the data flow diagram given below.

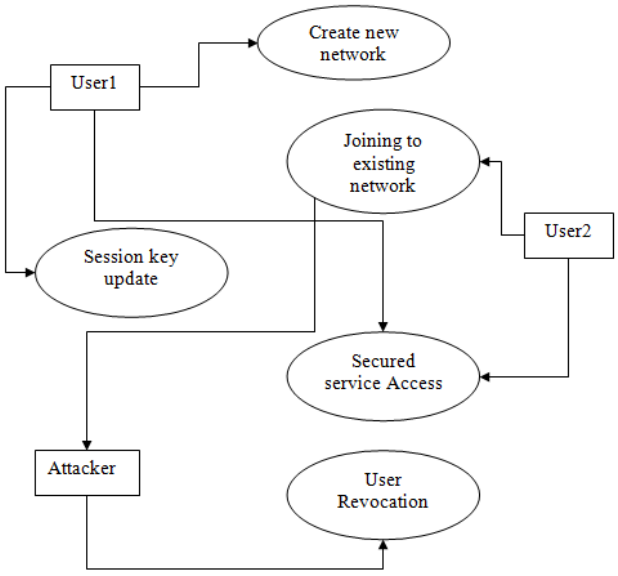

Figure 3. Data Flow Diagram for Network Formation

4. Protocol and Network Management

The user must determine whether to create a new network or participate in an existing one only after the validation/registration process of the user in the device has done. Services of the nodes starts only after the session key is generated and waits for the requests from other nodes if wanted to join the network. The node that belongs to the network responsible for validating new nodes data perform a diffusion process to the nodes within its communication range until the data reach all nodes in the network. This process allows verifying the validity and uniqueness of the new node's data. Several tasks are to be performed after the authentication of the node in which some of them are:

- Displaying the nodes (nodes/users).
- Updating/Modifying the trust of the nodes.
- Update the information of nodes present in the network.
- Process the request of certificates from other nodes.

4.1. Operation of Protocol

We used a model based on the asymmetric infrastructure of public keys which is mainly used for distributed and key management processes in order to provide defended connections. The protocol operates as follows:

Generation of IDC: Users provide their details in the registration process. After the registration process, users generate IDC. The IDC contains public and private components. It also contains the user's name, public key (Ki), the formation and expiration dates, an IP proposed by the user, and the user signature. The public component contains a Logical Identity (LID), which is unique for each user and allows nodes to identify it. Public, private key pair is generated using RSA algorithm.

Sharing IDC: A new user wants to join to the existing network. It executes Generation of IDC process initially. New user trusts the user in the existing network and provides its IDC encrypted using the public key the existing user. Existing user decrypts the IDC using private key.

Certificate Generation: Existing user authorizes the new user by providing certificate to the new user. Certificate consists of IDC with signature of the existing user. Signature is generated using the private key of the existing user. Existing user provides IDC and get certificate in the similar way as the new user.

Certificate Verification: When a user joined to the network, wants to access the services available in the network, the user gets the access only after the verification of the requesting user's certificate.

Defended Session Key Sharing: If the verification of the certificate is successful, then session key is shared to the requesting user defended by encrypting the session key using the public key the verification requesting user.

Defended Data Sharing: Service providing user encrypts the data using the session key using AES algorithm and sends it to Service requesting user. Service requesting user decrypts the data using session key.

4.2. Session Key Updation and Revocation

Session Key Update: Session key (Ks) have three fields: Formation time, session key and period. If the network initiated user detects that the session key is expired and required to be in the network even after expiration then user generates the new session key, encrypts it using the old session key and broadcast it to avoid duplications.

Session key Revocation: Session key has an expiration time, so it is revoked periodically. Session keys do not expire simultaneously in all nodes, instead avoids network flooding initiated by many nodes simultaneously when the session key is to be revoked. The life time of session key is

$$Ti = Fe - Fc \quad \text{where,}$$

Ti- lifetime of session key

Fe- Session key expiration time

Fc- Session key formation time

4.3. Malicious Node/User Revocation

Each user in the network maintains the revocation list. Revocation list contains the identity of the attackers. If a user is identified as the attacker, he/she should be eliminated from the network as shown in the figure above. Particular user's unique identity is

updated to the all the users existed in the network. All users in the network update their revocation list. When the attacker enters into the system for any service, revocation list is verified. If the user existed in the revocation list, that user will not get the service.

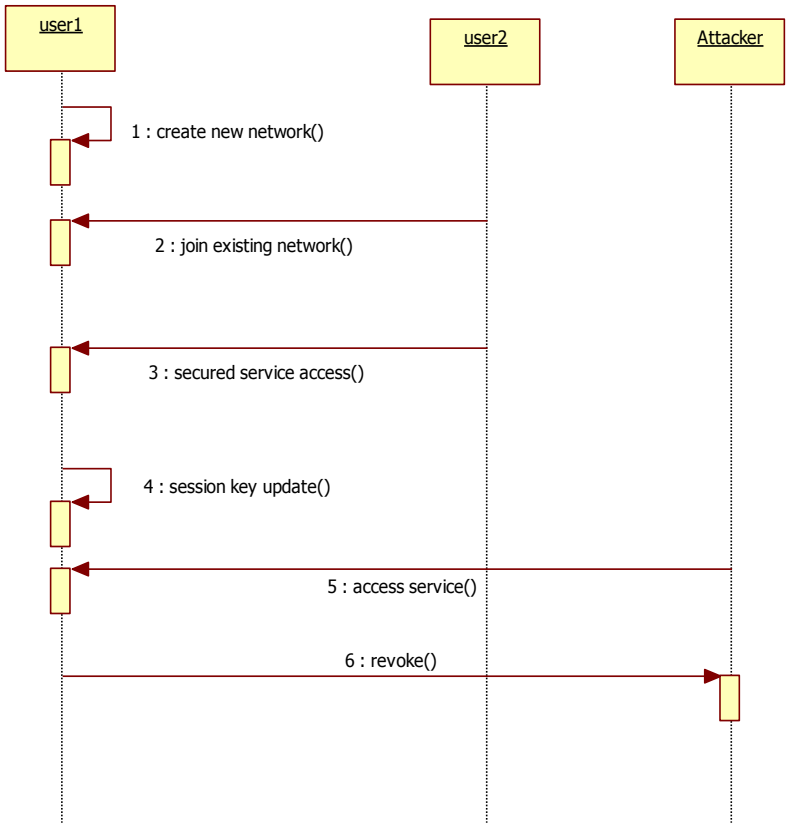

Figure 4. Clear View of Protocol Operation

5. Performance Analysis

The analysis is taken after running a set of tests to validate performance of the protocol operations. The protocol has been developed using Java programming, whose mobility, multi-platform, and interoperability, features are useful to deploy the protocol. The tests are carried out with a PC where all the nodes are joined/created virtually.

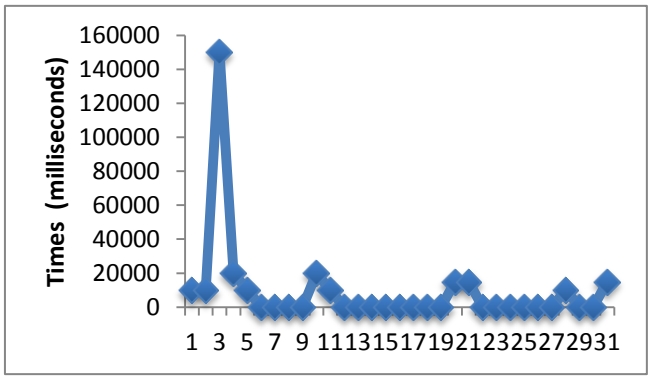

Figure 5. Runtimes Comparison (Cryptography c Operations)

Figure 5, shows the comparative graph of the measurements we have used in the nomenclature as: operation, algorithm used, key size, device, size of text *etc*.

We have grouped the data according to the type of operations: key formation, asymmetric encryption, symmetric encryption, asymmetric decryption, symmetric decryption, key signature and key verification.

The network is expected to be a small or medium-sized network, so it would require a small memory to work within the network. The devices running this protocol must have a minimum of volatile memory.

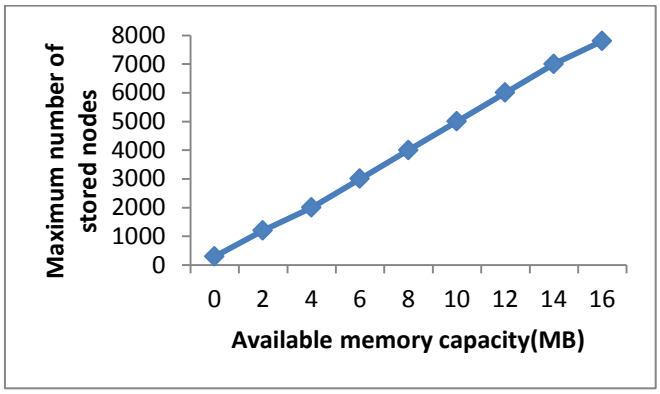

Figure 6. Maximum Numbers of Stored Nodes versus Available Memory

The above figure shows the maximum number of nodes that can be stored depending on the available memory capacity of the device when the percentage of memory availability for data storage is 30%.

5.1. Memory Consumption during Network Formation

The node that generates the network uses more memory because it is in charge of sending two messages for the authentication process, one with the symmetric encryption, and another with asymmetric encryption.

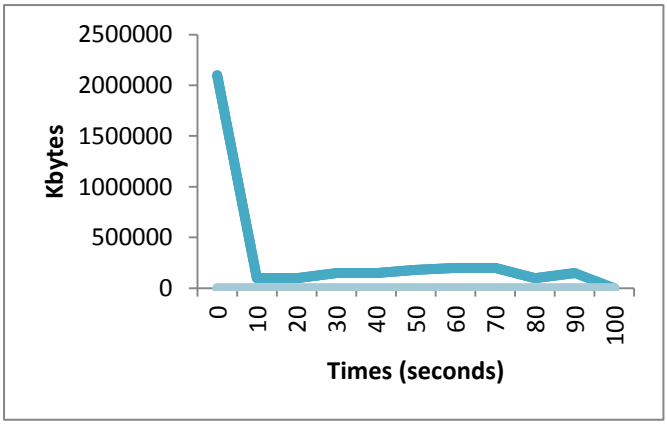

Figure 7. Memory used by Both Nodes from the Certificate Formation to the Data Transfer between them

The above figure shows the used memory, when a new node joins the network, by both nodes from certificate formation to data transfer.

6. Conclusion

Defended, autonomous the Passionate network has been proposed to be compatible for ad hoc networks. Session key has been use for defended communication. Authentication and authorization has been done using certificate. Symmetric key encryption has been used for data encryption. Asymmetric cryptography has been used for session key encryption and signature generation. Session key updating has been carried out based on expiration time. Revocation of the malicious user has been contributed.

References

[1] 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, no. 1/2, **(2012)**, pp. 1-8.
[2] V. Kumar and M. L. Das, "Securing Wireless Sensor Networks with Public Key Techniques", Ad Hoc and Sensor Wireless Networks, vol. 5, no. 3/4, **(2008)**, pp. 189-201.
[3] J. Goodman and A. Chandrakasanm, "An Energy Efficient Reconfigurable Public-Key Cryptography Processor Architecture", Proc. Int'l Workshop Cryptographic Hardware and Embedded Systems (CHES '00), **(2000)**, pp. 175-190.
[4] A. Wander, N. Gura, H. Eberle, V. Gupta and S. Chang, "Energy Analysis for Public-Key Cryptography for Wireless Sensor Networks", Proc. IEEE Third Int'l Conf. Pervasive Computing and Comm. (PerCom '05), **(2005)** March, pp. 8-12.
[5] M. Mukesh and K.R. Rishi, "Security Aspects in Mobile Ad Hoc Network (MANETs): Technical Review", Int'l J. Computer Applica-tions, vol. 12, no. 2, **(2010)** Dec., pp. 37-43.
[6] K. Sahadevaiah and P.V.G.D. Prasad Reddy, "Impact of Security Attacks on a New Security Protocol for Mobile Ad Hoc Networks", Network Protocols and Algorithms, vol 3, no. 4, **(2011)**, pp. 122-140.
[7] 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, **(2006)** Sept., pp. 567-585.