ISSN No. 0976-5697

Volume 5, No. 5, May-June 2014

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

# Group Key Regeneration for Improving Security in Spontaneous Wireless Ad hoc Networks

Aswini S
Department of Computer Science
NSS Engineering College Palakkad, India

Maya Mohan
Department of Computer Science
NSS Engineering College Palakkad, India

*Abstract:* Spontaneous networks are wireless ad hoc networks without fixed infrastructure and central administration. Security is the major concern in spontaneous networks because these networks will be created anywhere anytime according to user needs. Network communication is usually protected by the use of cryptography. This paper presents a security scheme which uses a hybrid cryptosystem to ensure secure communication. The scheme includes a new authentication protocol and a secure data transmission procedure. It uses public key infrastructure for authentication procedure. Initial trust establishment is based on the visual contact between users. Network traffic is protected by the use of a group key. For a node the fact of knowing the group key points out that it belongs to the network. Group key regeneration based on key use is also proposed in this paper. If the count on key use reaches the threshold value group key will be regenerated. Secure data transmission is based on the use of both public key infrastructure and symmetric key encryption. The proposed system improves the security requirements without increasing the communication cost. It also reduces the computation time and energy requirements for data encryption/decryption. The proposed system has been implemented using java programming. A security analysis of the system is also included in this paper.

*Keywords:* Security; Authentication; Wireless Network; Spontaneous network; public key infrastructure; symmetric encryption

## I. INTRODUCTION

Mobile ad hoc networks are infrastructure-less networks with no central administration. Due to this nature of MANETs, they are more desirable medium of communication in environments like disaster relief, battle fields or traffic control. Spontaneous network is a subset of ad hoc network. Its main objective is the integration of services and devices into network environments with instantaneous service availability without any manual intervention [1]. By their nature, they have a limited extent in both space and time and following human interactions [2]. Since it is a wireless network, securing communication over this network is a challenging task.

Performing communication in free space exposes spontaneous networks to attacks because anyone can join the network, and eavesdrop or inject messages [3]. In spontaneous networks, communication takes place among groups having some common objective. The communication must be made reliable in regards of security, data transfer from node to node and quality of service. For this, it is necessary to employ security mechanisms that ensure that only authorized nodes can inject traffic into the network.

Cryptographic algorithms play an important role in the security management of spontaneous networks. All the existing security schemes are based on either asymmetric public key infrastructure or symmetric key encryption. A hybrid scheme which relies on both public key infrastructure and symmetric algorithms is more efficient. The existing methods like predistribution key algorithms [4] and dynamic threshold crypto systems [5] are not suited for spontaneous networks because this is a fully self organized network without preconfiguration. Some systems rely on trusted authorities for proper authentication [6]. Spontaneous network security does not rely on any trusted authority or fixed server.

In this paper a new hybrid scheme is proposed to improve the security in spontaneous networks. Here the security management scheme consists of an authentication procedure and a secure data transmission procedure. Authentication is based on the asymmetric public key infrastructure. Group traffic is protected by using symmetric encryption. Group key regeneration based on the use of the key is also included in this paper. Asymmetric cryptography is used to transfer the key generation material. Initial trust establishment is based on the visual contact between users and a distributed certification authority is also used for trust establishment. Secure data transmission also uses symmetric encryption. The proposed scheme is better than the existing systems in terms of energy consumption, scalability and security.

The rest of the paper is organized as follows. Section 2 gives the related works on security in spontaneous networks. The proposed system is explained in Section 3. Section 4 gives the security analysis of the proposed system. Section 5 shows the implementation details and simulation results. Section 6 gives the conclusion.

## II. RELATED WORKS

R. Lacuesta, J. Lloret, M. Garcia, and L. Pen alver propose a secure spontaneous ad-hoc network, based on direct peer-to-peer interaction, to grant a quick, easy, and secure access to the users to surf the web in [7]. Their security scheme is based on the asymmetric cryptography. They has also given protocol procedures and messages to be followed to transfer data. Analytical and simulation models are also proposed in this paper.

In [8] L.M. Feeney, B. Ahlgren, A. Westerlund, and A. Dunkels have proposed Spontnet, a prototype implementation of a simple ad hoc network configuration utility based on basic concepts of spontaneous networking. Here much of the network configuration infrastructure is derived from the face to face human interaction patterns. Spontnet allows users to distribute a group session key without previous shared context and to establish shared namespace. They also provide examples of collaborative applications that could be useful in a spontaneous networking environment.

In [9] M. Danzeisen, T. Braun, S. Winiker, D. Rodellar described the implementation architecture with the objective of enabling secure spontaneous networking in a user friendly way. Implementation leverages a dashboard-like tool, which can, with the help of a cellular network, ease the formation of spontaneous networks among heterogeneous nodes. Initial configuration and security parameter exchange is done with the help of cellular networks. They also defined a Bluetooth scenario, where they presented a mechanism to resolve communication addresses to primary identifiers using service discovery attributes.

Raquel Lacuesta, Jaime Lloret, Miguel Garcia, Lourdes Penalver proposed a secure protocol for spontaneous wireless adhoc network creation [10]. Here, the authentication procedure is based on asymmetric public key infrastructure and communication is protected by the use of a session key. This is a complete self-configured secure protocol, which describes network creation and secure sharing of services without any infrastructure.

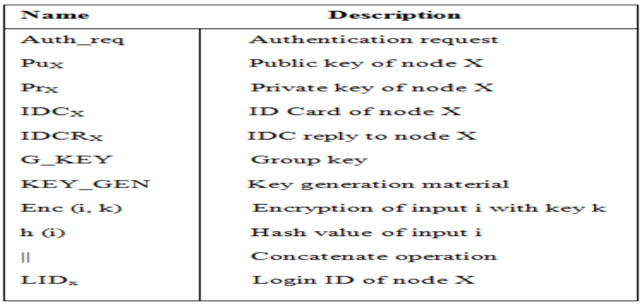
Sencun Zhu, Shouhuai Xu, Sanjeev Setia, and Sushil Jajodia describe a lightweight hop-by-hop authentication protocol for ad-hoc networks [11]. This protocol is based on hop-by-hop authentication for verifying the authenticity of all the packets transmitted in the network and one-way key chain and TESLA for packet authentication and for reducing the overhead for establishing trust among nodes.

## III. PROPOSED SYSTEM

### *A. Spontaneous Network Creation:*

Spontaneous network is created when a group of people come together to carry out a specific task. In this case, we can use human interactions associated with the group communication in order to establish the configuration infrastructure. First, a node will create the spontaneous network and generates a group key, which will be exchanged with new nodes after the authentication phase. The key will protect the network traffic by encryption and allows each node to authenticate itself as a group member. First node is also responsible for the initial network configuration (SSID, IP configuration, Protocol ...). Since it is a self organized network, each node must configure its own data (IP, port, data security). The nodes in the network and services may vary because devices are free to join or leave the network. Table I describes the notations used in the proposed system.

Table I. Notations used in proposed system



| Name | Description |
|---|---|
| Auth_req | Authentication request |
| $Pu_X$ | Public key of node X |
| $Pr_X$ | Private key of node X |
| $IDC_X$ | ID Card of node X |
| $IDCR_X$ | IDC reply to node X |
| G_KEY | Group key |
| KEY_GEN | Key generation material |
| Enc (i, k) | Encryption of input i with key k |
| h (i) | Hash value of input i |
| \|\| | Concatenate operation |
| $LID_x$ | Login ID of node X |

### *B. Authentication Procedure:*

The authentication mechanism proposed in this paper ensures that only authorized nodes can inject traffic into the network. Here only authenticated nodes are allowed to participate in the network.

In this system each node who wishes to join the network should possess an identity card (IDC) which contains all the necessary information about the node. An ID card contains logical ID, public key of the node, IP address proposed by the node and information signature. User signature is generated using SHA-1on the previous data. Then this will be signed with private key of the owner of IDC. When a new node wants to join the network, it has to exchange its IDC with the first node. And the new node should be visible to the first node. Because the initial trust establishment is based on the visual contact between users. Use of short-range technologies (Bluetooth) for authentication improves the security of the system,

Authentication procedure is based on the use of asymmetric public key infrastructure. Fig.1 shows the authentication procedure. Consider a new node B wants to join the spontaneous network created by the node A. First B will send an authentication request to A. A will reply with its public key. Then B will send its ID Card encrypted with A's public key. A will validates B's ID Card and verifies the information signature in order to ensure that the data has not been modified. In this step, A establishes the trust level of B by looking physically at B. It depends on whether A knows B or not. If a decides to trust B it will send its ID Card encrypted with B's public key. B will also verify the information signature and validates the data. Now, A and B will trust each other. In order to assign an IP address to B, A has to check whether there is another device in the network with the same IP. It helps to avoid IP duplication. After that B has to agree on the protocol and speed of the network. Then A will send the initial session key and key generation material encrypted with B's public key to B. Similarly each additional node authenticates with any of the existing node in the network. This session key not only used to protect the group traffic but also to define network boundaries for the group.

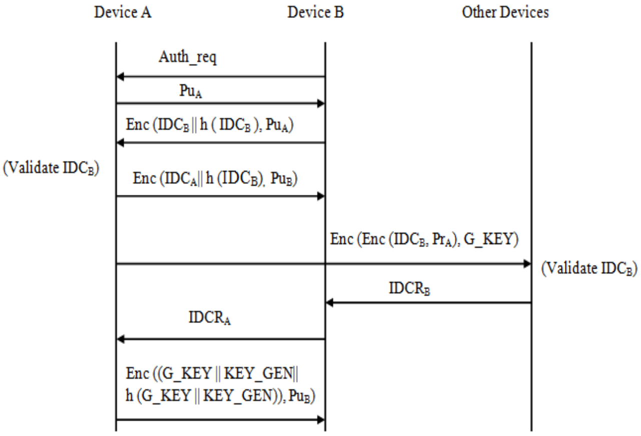

Device A
Device B
Other Devices
Auth_req
$Pu_A$
Enc ($IDC_B$ || h ( $IDC_B$ ), $Pu_A$)
(Validate $IDC_B$)
Enc ($IDC_A$|| h ($IDC_B$), $Pu_B$)
Enc (Enc ($IDC_B$, $Pr_A$), G_KEY)
(Validate $IDC_B$)
$IDCR_B$
$IDCR_A$
Enc ((G_KEY || KEY_GEN||
h (G_KEY || KEY_GEN)), $Pu_B$)

Figure 1. Authentication procedure for a new node

### *C. Se cure Communication:*

An authenticated node can access data, services and resources provided by other nodes in the network. Also it can allow access to its services and resources. The user has to ask other network members to know the available services. An authenticated node is able to modify the trust of other network members. Trust modification is needed only when a node seems compromised.

Network communication is usually protected by the use of cryptography. Some of the existing data transfer schemes are based on public key infrastructure. But it will be time consuming and energy consuming when we needs to transfer large volume of data. So a new secure data transmission scheme is described in this section.

Here a symmetric encryption scheme using a group key is proposed to secure the broadcasting of information. The group key will have an expiration time based on its use. After that the key should be updated. Fig.2 shows the encryption using group key and key regeneration.

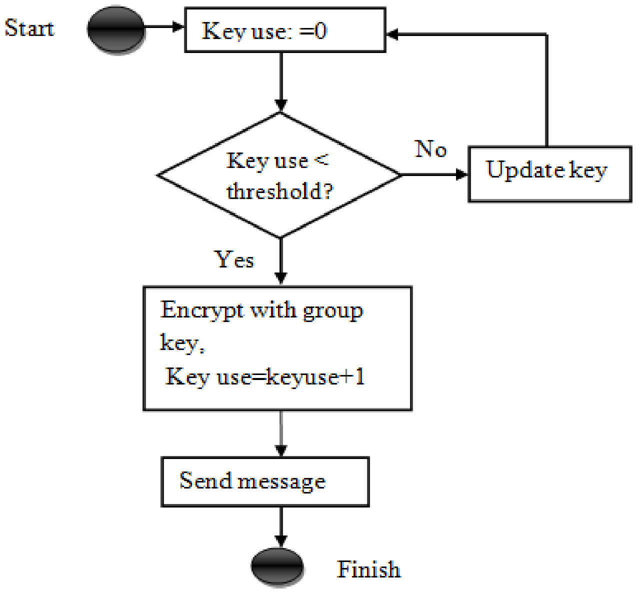


Figure 2. Encryption and group key generation

### a. *Group Keu Formation and Regeneration:*

In this system initial group key is generated by the creator node. Key regeneration is based on the use of group key. Here each node will have a local counter to count the use of group key. Counter is incremented each time the node uses the session key. If the value goes above the pre defined threshold, the node has to send key update message to all other nodes in the network along with a certificate to prove his identity. After the verification of the message all nodes in the network will independently generate the new group key.
New G_KEY= h (KEY_GEN || Old G_KEY)

## IV. SECURITY ANALYSIS

Security means protecting the privacy, availability, integrity and non-repudiation and identifying potential attacks from unauthorized access, use, modification or destruction.

The proposed scheme is based on the following assumptions.

a. Only known nodes can enter into the network.
b. Each node should be visible to at least one of the existing nodes in the network.
c. All the nodes should establish trust with all other nodes in the network.
d. User device should be protected with a password

The attacks on the spontaneous networks can be passive and active attacks. A passive attack attempts to retrieve the data by listening to traffic channel without proper authorization, but does not alter the data. An active attack attempts to modify the system resources. It involves information interruption and modification.

The main aim of providing security is that, the system should not be vulnerable to attacks, which will leads to data loss or privacy problems.

How the proposed system prevents the usual attacks is given below:-

***a)*** ***Passive eavesdropping:*** - Here the attacker tries to discover information by monitoring the network traffic. But in the proposed system group traffic is protected by AES symmetric encryption. Here group key is used as the symmetric key. It will be regenerated based on its use.

***b)*** ***Man-In-The-Middle Attack:-*** In this attack, the attacker exists as a neighbour to any one node in the transmission path and tries to alter data. It is prevented by the use of hash functions (data integrity checking). Also short range communication technologies are used for data transfer. Group key regeneration also helps to prevent this.

***c)*** ***Impersonation attacks:*** - Proposed system uses the visual identity verification for trust establishment. Use of short range technologies for authentication also prevents this type of attacks.

***d)*** ***Active spoofing attacks:-*** The proposed scheme will check for IP duplication at the time of authentication, it will prevent IP spoofing attacks. Hashing is used to check data integrity.

***e)*** ***Brute-Force attack:-*** This is a key guessing attack. Here group key will be regenerated based on its use. It will make it difficult to launch brute-force attack.

***f)*** ***Compromised physical device:-*** User device is protected by password. Visual identity verification and trust modification also helps to prevent this.

## V. SIMULATION RESULTS

The proposed system has been implemented using java programming. Software simulation of spontaneous network is obtained using Netbeans IDE. Profiling tools are used to monitor the memory usage and computation time of the encryption algorithms. Fig. 3 shows the computation time of AES and RSA algorithms.

Performance of encryption algorithm is evaluated considering the memory usage, computation time, output bytes in [12].Time taken by RSA algorithm is much higher compare to the time taken by AES algorithm. It shows that AES is better than RSA in terms of memory usage and computation time. So we will replace the public key Cryptography by symmetric key encryption. Simulation results show that the proposed system doesn’t increase the computation time and energy requirements.

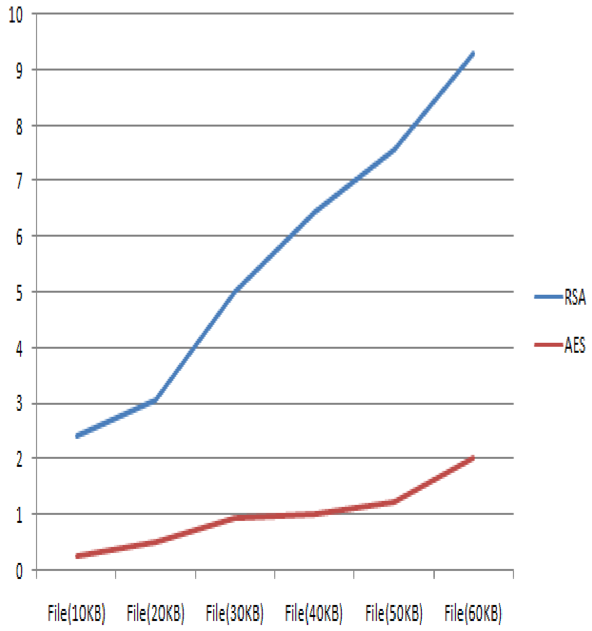


Figure 3. Computation time comparison of RSA and AES

## VI. CONCLUSION

Spontaneous wireless ad hoc networks are temporal networks, created to perform some collaborative activities. It is an infrastructure less, dynamic network with a group of self configured nodes. Initial network configuration is based on human interaction pattern. The main objective of the proposed system is to provide secure communication in spontaneous networks without increasing the communication costs. The system allows sharing resources and offering new services among users in a secure way. So here a scalable, hybrid security scheme with an authentication procedure and secure communication is proposed. The analysis on existing systems and simulation results shows that the proposed system improves the security of communication over spontaneous network without increasing the computation time and energy requirements.

## VII. REFERENCES

[1] S. Preuß and C.H. Cap, “Overview of Spontaneous Networking -Evolving Concepts and Technologies”, Rostocker Informatik-Berichte, 2000.

[2] L.M. Feeney, B. Ahlgren, and A. Westerlund, “SpontaneousNetworking: An Application-Oriented Approach to Ad-hocNetworking,” IEEE Comm. Magazine, June 2001.

[3] M. Mukesh and K.R. Rishi, “Security Aspects in Mobile Ad Hoc Network (MANETs): Technical Review,” Int’l J. Computer Applications, Dec. 2010.

[4] 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.

[5] A. Noack and S. Spitz, “Dynamic Threshold Cryptosystem without Group Manager,” Network Protocols and Algorithms, Oct. 2009.

[6] 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.Sept.2007.

[7] R. Lacuesta, J. Lloret, M. Garcia, and L. Pen˜ alver, “A SpontaneousAd-Hoc Network to Share WWW Access,” EURASIP J. WirelessComm. and Networking, 2010.

[8] ] 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.

[9] Raquel Lacuesta, Jaime Lloret, Miguel Garcia, and Lourdes Pen˜ alver-“ A Secure Protocol for Spontaneous Wireless Ad Hoc Networks Creation”- IEEE Transactions On Parallel And Distributed Systems, April 2013.

[10] Raquel Lacuesta, Jaime Lloret, Miguel Garcia, and Lourdes Pen˜ alver-“ A Secure Protocol for Spontaneous Wireless Ad Hoc Networks Creation”- IEEE Transactions On Parallel And Distributed Systems, April 2013.

[11] S. Zhu, S. Xu, S. Setia, and S. Jajodia, “LHAP: A Lightweight Hopby-Hop Authentication Protocol For Ad-Hoc Networks,” Ad HocNetworks. Sept. 2006.

[12] Diaa Salama Abd Elminaam, Hatem Mohamed Abdual Kader, and Mohiy Mohamed Hadhoud. Evaluating the Performance of Symmetric Encryption algorithms, International Journal of Network Security, May 2010 .