www.ijecs.in
International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 5 Issue 12 Dec. 2016, Page No. 19419-19428

Enhanced Security Protocol for Spontaneous Wireless ad-hoc Network

Firoj*, Ravi Antil, Ankur Jain
M.Tech,ECE Deptt.,MSIT,sonepat
Firozmirza786@gmail.com
A.P,ECE Deptt.,MSIT,Sonepat
antilravi6519@gmail.com
A.P,ECE Deptt.,MSIT,Sonepat
ankurjain797@gmail.com

Abstract— *with continual advances in technology, coupled with increasing price/performance advantages, wireless accessibility is being deployed increasingly in office and public environments. This paper discusses the security threats and risks associated with wireless networks, and outline a number of best practices for deploying wireless networks in corporate and home environments. Finally, an Enhanced 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. Proposed protocol is secure autonomous protocol and is not based on any infrastructure and external support in order to develop it over the devices with limited resources. Network creation, communication and management are the functionalities of the proposed system. A mechanism has been presented to allow the nodes to check the authenticity of their IP addresses while not generating any duplicated IP addresses. This mechanism helps nodes to authenticate by using their IP addresses. The proposed protocol has the following features Distributed security mechanism, Lightweight, Malicious user revocation capability.*

Keywords— NS-2, IDC, Wireless Network, IEEE,PDR

I. INTRODUCTION

Wireless networks represent a rapidly emerging area of growth and importance for providing ubiquitous networking connections. The common technologies can be classified into different categories according to the range of the service area. On a worldwide scale, telecommunication companies have been making significant progress in carrying voice and data traffic over their cellular networks; furthermore, the next generation infrastructure, under development all over the world, aims to provide higher bandwidth and better quality for multimedia traffic. In a metropolitan area, WiMAX (IEEE 802.16) can provide users with high-speed broadband access to the Internet. In a local area, WiFi (IEEE 802.11) enables users to establish wireless connections within a corporate or campus building. Moreover, in a personal area (often less than 10 meters), Bluetooth (IEEE 802.15) can provide low-cost and short-range connectivity for portable devices.
In a general network system, security has different contexts depending on different applications, among which the essential requirements are data confidentiality and integrity, authentication, and availability.

Data Confidentiality and Integrity The network MUST provide strong data confidentiality, integrity, and replay protection for every transmitted message. Data confidentiality and integrity, helping build a secure channel for the user to communicate in an insecure environment, mean that only the communicating users are able to understand the received messages, generate or modify valid messages. Furthermore, replayed messages should be recognized and discarded even though they may pass the integrity check. These requirements could be satisfied by well-designed cryptographic functions and appropriate replay protection techniques.

Mutual Authentication The network MUST provide mutual authentication, which means that the communicating peers authenticate each other's identity. If required, the authentication process should also combine with key generation, distribution and management to provide secret keys for the cryptographic

function. Based on the authentication results, flexible authorization and access control policies could be deployed to restrict the privilege of users.

Availability is a form of robustness, which is another important category of security requirements. The network should be able to prevent an adversary from shutting down the connectivity for a legitimate individual or the entire system. In other words, Denial of Service (DoS) attacks should be eliminated, or at least mitigated.

Some of the advantages of spontaneous wireless ad-hoc network are as follow:

Lightweight Protocol

As these networks are implemented in devices such as laptops, PDAs or mobile phones, with limited capacities thus they must use lightweight protocols and new methods to control, manage, and integrate them. The 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 behaviour 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.

Security Features

Confidentiality, Node cooperation, anonymity and privacy.

Constraints
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.

Services
Group communication, collaboration in program delivery, security.

II. LITERATURE REVIEW

Ronald Watro, "TinyPK: Securing Sensor Networks with Public Key Technology" 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.
Raquel Lacuesta , "A Spontaneous Ad Hoc Network to Share WWW Access" A secure spontaneous ad-hoc network is presented, which is based on direct peer-to-peer interaction, to grant a quick, easy, and secure 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.
James Goodman, "An Energy-Efficient Reconfigurable Public-Key Cryptography Processor"
Given a specific domain of functionality such as public-key cryptography, it is possible to provide a limited degree of domain-specific re-configurability to provide flexibility while minimizing the overhead that is typically associated with reprogrammable logic. Domain specific integrated circuits (DSICs) utilize

interconnect-centric architectures to exploit locality in order to minimize the interconnection overhead, which is the dominant source of energy consumption in generic reconfigurable logic.

Arvinderpal S. Wander, "Energy Analysis of Public-Key Cryptography for Wireless Sensor Networks"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 un-trusted parties are considered such as two nodes in a wireless sensor network.

J. Latvakoski, D. Pakkala, and P. Paakkonen explained communication architecture concept for spontaneous systems. The concept integrates application-level spontaneous group communication and ad hoc networking together. A service gateway is used to connect multiple technologies and networks together. A set of methods to enable plug and play, addressing and mobility, peer to peer connectivity and use of services are also provided.

III. PROPOSED WORK

A simple security model for a sensor network employees a single secret key that is known by all nodes in the sensor network. There are many potential problems with this simple model and it clearly fails to scale to large systems. However, in a small local region of the sensor network, this simple model is likely to hold. The single shared secret key creates a communication crypto net: possession of the key authenticates the holder as part of the secure group. Traffic sent in the sensor network is encrypted and integrity protected using the common key. Since traffic is sometimes broadcast and sometimes routed hop-to-hop across the sensor network, the single encryption key provides very user friendly security architecture, albeit with the already mentioned limitations. This system uses the Centralized authority which affects the spontaneous nature of the network.

None of the existing systems propose a secure spontaneous network protocol based on user trust that provides node authenticity, integrity checking, and privacy and they require an initial configuration (i.e., network configuration) or external authorities (for example, central certification authorities). To solve the above issue, a novel protocol is proposed for the creation of spontaneous network and data distribution, sharing of resources, and services securely. Main objective of the spontaneous network creation is the integration of services and devices in the same environment, enabling the user to have instant service without any external infrastructure.

Proposed protocol is more secured and autonomous protocol which is not based on any infrastructure and external support in order to develop it over the devices with limited resources. Network creation, communication and management is the functionalities of the proposed system.

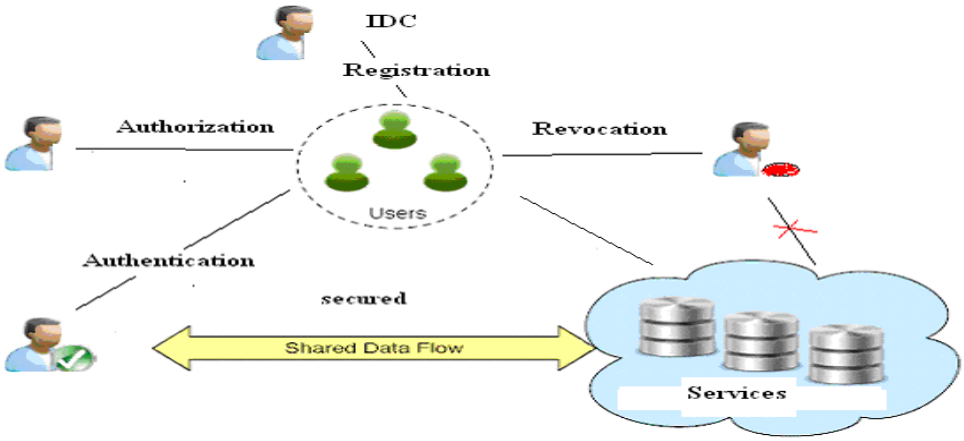

Fig 1: Secured Wireless Ad hoc Network

Initial data and key exchange is done based on trust between nodes. Data is exchanged securely by applying encryption over the data with key. 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. Security is established based on the service required by the users, by building a trust network to obtain a distributed

certification authority. A new user can be joined to the network only if he/she knows someone who belongs to the network. Certificate authority is distributed between the users who trust the new user. The network management is also distributed, which allows the network to have a distributed name service.
The proposed protocol has following features:

- Distributed security mechanism
- Lightweight
- Malicious user revocation capability

Malicious 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. 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.

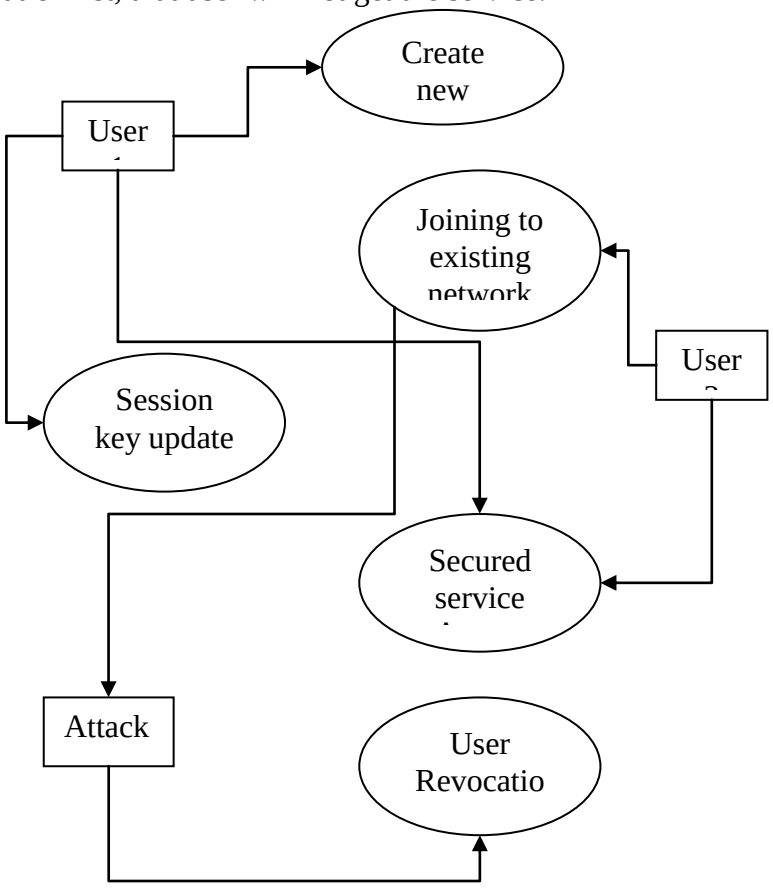

Fig 2: Flow chart of spontaneous secured network

Ad hoc network is basically infrastructure less in nature and it is vulnerable to attacks. In such a network it is necessary to create the security without autonomously and without the involvement of centralized architecture. To solve the above issue, a novel security protocol is proposed for the spontaneous network creation. Initial network creation is 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 secure 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. Hence security is enhanced with revocation capabilities.

DOI: 10.18535/ijecs/v5i12.27

The presented work is divided in five stages:

1. Creating a new Network

1a.Generation of IDC

1b.Generation of session key

2. Joining to the existing network

2a.Sharing IDC with signature using Cryptography algorithm

2b.Authorization: Certificate Generation to the new user

3. Service Access

3a.Authentication: Certificate Verification

3b.Secure session key sharing

3c.Secure Data Sharing

4. Session Key Update

5. User Revocation

IV. IMPLEMENTATION

The enhaced secured Protocol is implemented with the help of Network Simulator NS-2.35.Which is widely used simulation tool for wireless Network.

The proposed algorithm is simulated in following steps

1. Creating a new Network

1a.Generation of IDC

1b.Generation of session key

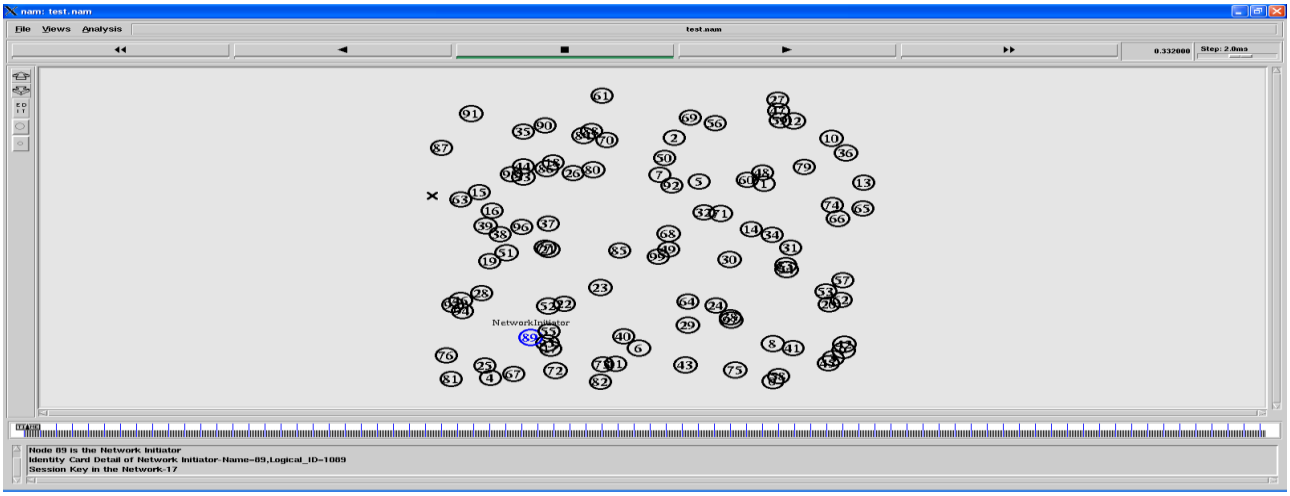

Fig 3: Generation of IDC and session key

Here figure 4.4 showing the data generation of IDC and session key over the network. The figure is showing that for creating a secured spontaneous network between the node pair of the network, node 89 acts as a network initiator, who will create a spontaneous network while session key is initiated by the node 17, which will be exchanged with new nodes after the authentication phase.

2. Joining to the existing network

2a.Sharing IDC with signature using Cryptography algorithm

Here figure 4 is showing that the requested IDC is shared with all the existing members of the network with signature by using cryptography algorithm. The above figure depicts that node 6 wants to joins the network therefore submit its IDC to network Initiator. Thereafter network member will encrypted the IDC and provide authentication and again network initiator will decrypts the member IDC for providing security in the network.

DOI: 10.18535/ijecs/v5i12.27

Network Member: 2
Name (6)=6

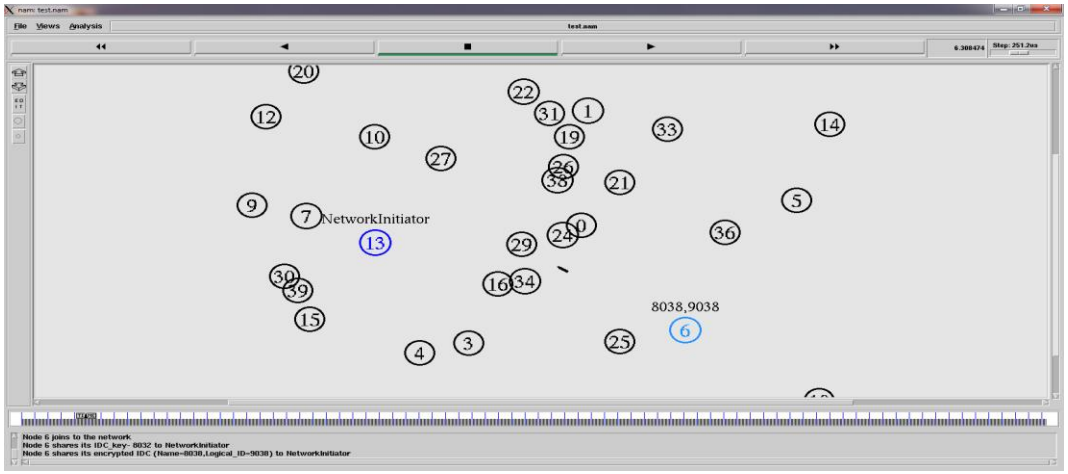

Fig 4: sharing of IDC using Cryptography algorithm

Logical_ID (6)=1006
IDC key = 8032
Encrypted IDC:
Name=8038
Logical_ID=9038
Network Initiator decrypts the member IDC
Decrypted IDC:
Name=6
Logical_ID=1006

2b.Authorization: Certificate Generation to the new user

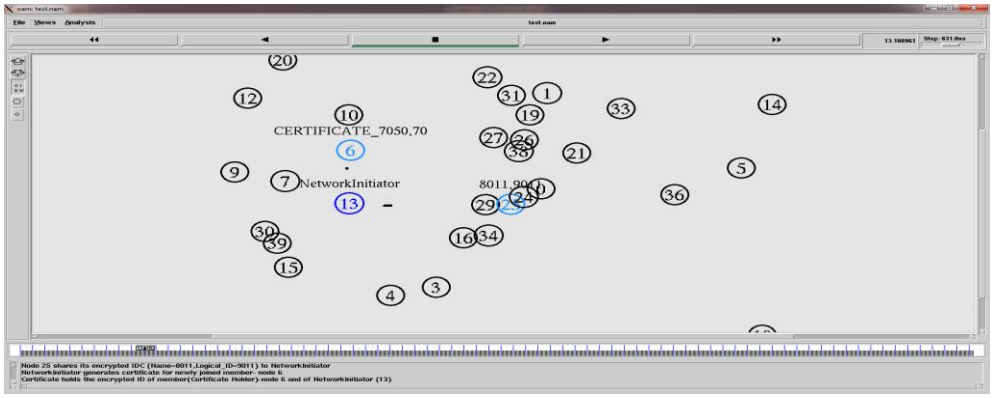

Fig 5: certification generation to the new user

Here figure 5 is showing that after verifying the network member, network Initiator decrypts the Encrypted IDC using the IDC key and when the decrypted IDC name is equal to the network member, network Initiator generates certificate for newly joined member. Thus certificate of validate IDC is issued by network initiator. Certificate holds the encrypted ID of member (Certificate Holder) and of Network Initiator (Issuer).
Certificate of member: 6
Signing Key=7037
Issuer=7050
Holder=7043

3. Service access

3a.Authentication: Certificate Verification.

DOI: 10.18535/ijecs/v5i12.27

3b.Secure session key sharing
3c.Secure Data Sharing

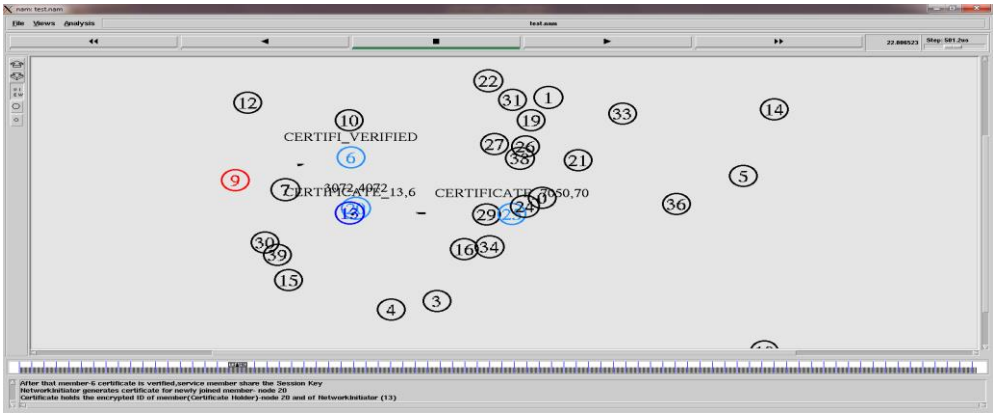

Fig 6: verification of issued certificate

Here figure 6 is showing that the Service providing user encrypts the data using the session key using symmetric encryption algorithm and sends it to Service requesting user. Service requesting user decrypts the data using session key.
When network member node 6 (Requesting service member) gets the service from the any service member, first submitting the certificate to service member (node-25).
The service member (node-25) verifies the certificate of requesting service member 6.
If the verification of the Requesting member certificate is successful, it provided the service to its corresponding Requesting member node 6.
Requesting_Service_Member:6
Service_Member of node-6:25
Certificate_Verification of member: 6
Decrypted_Issuer=13
Decrypted_Holder=6

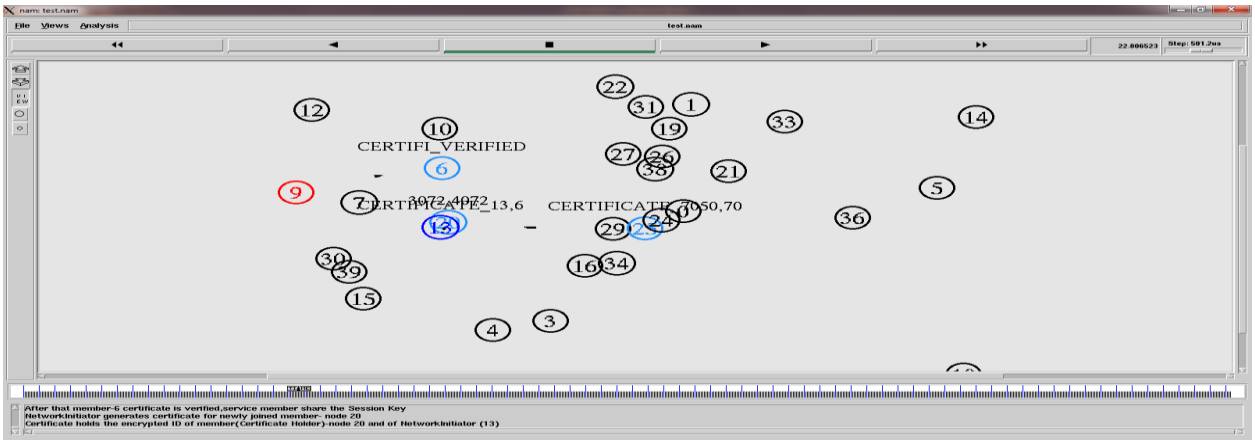

Fig 7 Verification of Certificate

Here figure 7 is showing that after verification of certificate, service is provided to the requested node. Here service member 25 is verified the certificate of request member (node 6), then it's provide the service to request member node 6.
During the service (data) transmission, the data must encrypt and send to the corresponding request member (node 6). The data will be encrypted using the shared session key.
When the corresponding request member (node 6) received the encrypted data, it decrypts the data using the same session key.
Service_Member_25_DATA

DOI: 10.18535/ijecs/v5i12.27

DATA:cefvfwqtpi
Encrypted Text:
dfgwgxruqj
Requesting_Service_Member_6 (Access the data from node 25)
Decrypted Text:
cefvfwqtpi

PERFORMANCE ANALYSIS

Normalized routing overhead

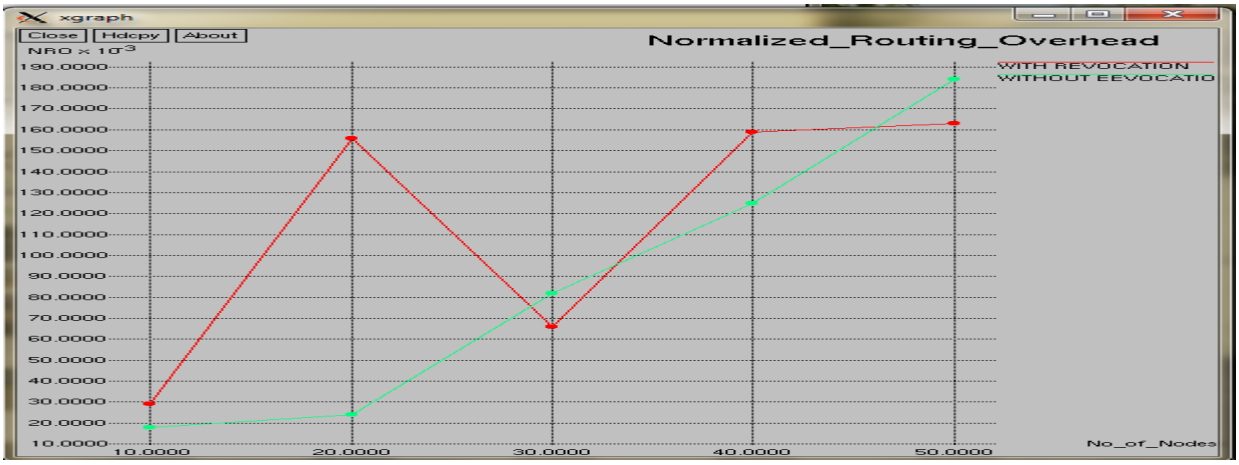

Fig 8: Normalized Routing Overhead Vs Number of Nodes

Here figure 8 is showing that Normalized routing Overhead with revocation is higher than that Normalized routing Overhead of without revocation. Because with revocation as the new user has to share control information for secure data services. Normalized routing overhead is more as compare to without revocation.

Throughput

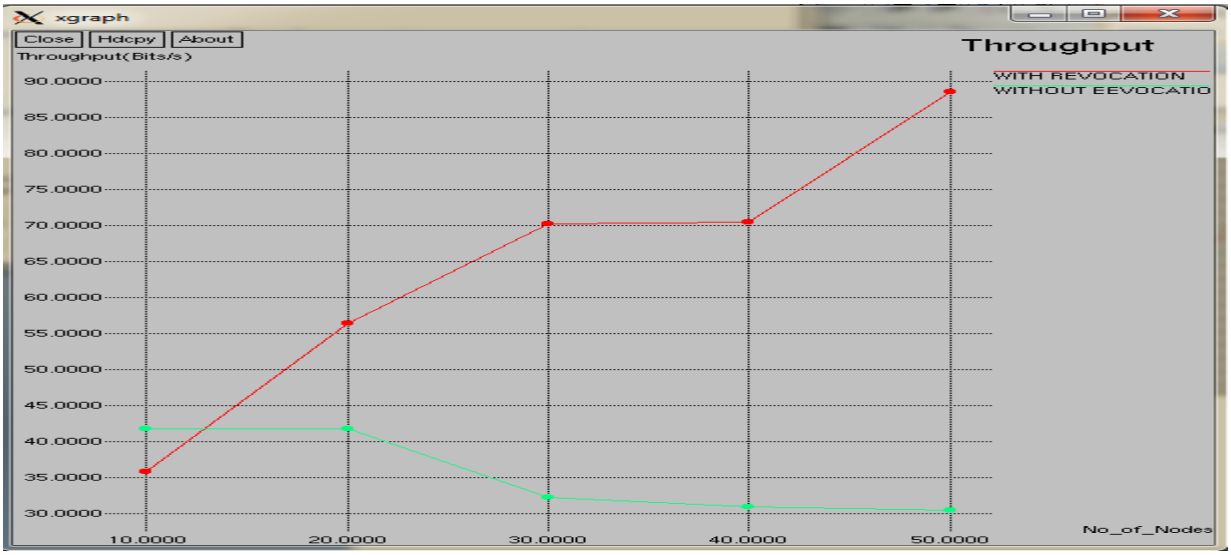

Fig 9: Throughput Vs Number of Nodes

Here figure 9 is showing that throughput of with revocation is higher than that of throughput of without revocation. In with revocation, when the attacker is detected, it eliminates the attacker in the network. Therefore attackers will not involve in the future.

DOI: 10.18535/ijecs/v5i12.27

Packet Delivery Ratio

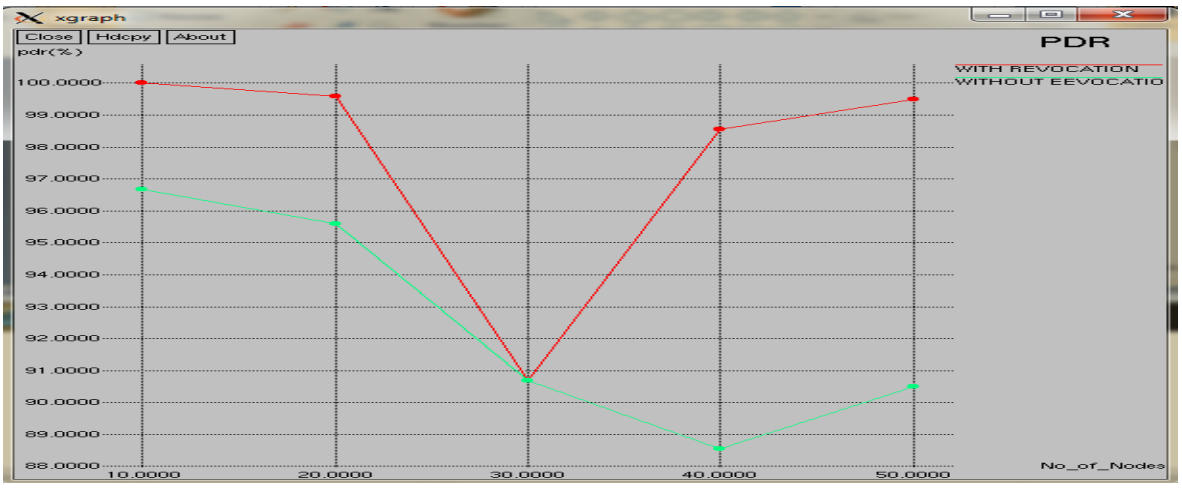

Fig 10: PDR Vs Number of Nodes

Here figure 10 is showing that Packet Delivery Ratio of with revocation is higher than that of Packet Delivery Ratio of without revocation. Because in without revocation list mechanism, the attacker is only detected, but it not eliminated from the network. Therefore a chance to this attacker affects the network. Thus if revocation list mechanism is used then attacker not only detected but is also removed from the network. Therefore Packet Delivery Ratio with revocation is better than without revocation.

Average Delay

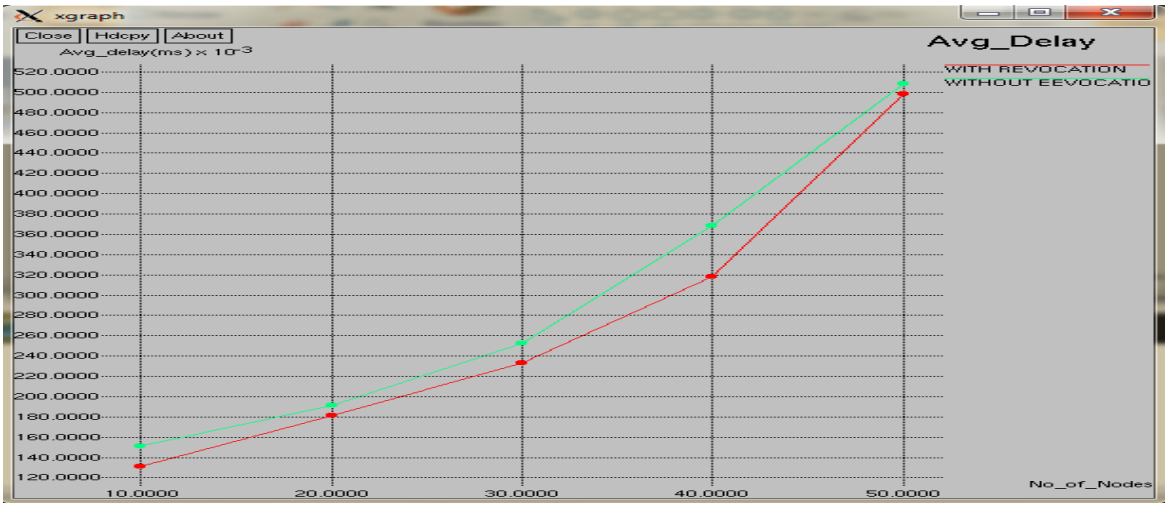

Fig 11: Average Delay Vs No. of Nodes

Here figure 11 shows that Average Delay of with revocation is lower than that of Average Delay of without revocation. Because in without revocation, the attacker is detected, but it not eliminated from the network. Therefore a chance to this attacker affects the network and causes a delay. Thus Average delay with revocation shows better result than without revocation.

CONCLUSION

In this paper, we show the design of an enhanced 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 enhanced the previous work by adding revocation method. We

have also simulated the enhanced protocol of spontaneous network with revocation and without revocation and checked the performance of both with respect to packet delivery ratio, throughput, average delay, Normalized routing overhead and finds that with revocation method protocol performs better with respect to without revocation. 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).

REFERENCES

[1] Raquel Lacuesta, Jaime Lloret, Senior Member, IEEE, A Secure Protocol for Spontaneous Wireless Ad Hoc Networks Creation IEEE transaction on parallel and distributed systems, vol. 24,no. 4,april 2013

[2]. 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.

[3]. 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.

[4]. 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.

[5]. 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), Aug. 2004.

[6]. 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.

[7]. 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.

[8]. J. Rekimoto, "SyncTap: Synchronous User Operation for Spontaneous Network Connection," Personal and Ubiquitous Computing, vol. 8, no. 2, pp. 126-134, May 2004.

[9] R. Lacuesta and L. Pen˜ aver, "IP Addresses Configuration in Spontaneous Networks," Proc. Ninth WSEAS Int'l Conf. Computers (ICCOMP '05), July 2005

[10]. 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.

[11]. 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.

[12]. R. Lacuesta, J. Lloret, M. Garcia, and L. Pen˜ alver, "Two Secure and Energy-Saving Spontaneous Ad-Hoc Protocol for Wireless Mesh Client Networks," J. Network and Computer Applications, vol. 34, no. 2, pp. 492-505, Mar. 2011.