Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 5, May 2014, pg.758 – 768

RESEARCH ARTICLE

Secure Protocol and Signature Based Intrusion Detection for Spontaneous Wireless AD HOC Network

Nikhil Varghane[1], Bhakti Kurade[2]

[1]Computer Science and Engineering, G.H. Raisoni Academy Of Engineering, India

[2]Computer Science and Engineering, G.H. Raisoni Academy Of Engineering, India

[1] n.varghane@gmail.com; [2] Bhakti.Kurade@Raisoni.net

Abstract— Network security become important aspect in wireless network creation &wireless communication so we proposed a complete independent self-configured network creation there is no need any fixed infrastructure as well as no need any central administrator to handle the services and share the secure data and there is no need any external support for handling the functionality of the network. Proposed a secure protocol for spontaneous wireless ad hoc networks which uses a hybrid public, private key 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. The protocol offers Network creation, protocol messages, and network management communication intrusion detection. We presenting self-configured secure protocol that is able to create the network and share networks secure services. The network allows sharing resources and new services among users in a secure environment. Likewise In this paper we focus on intrusion detection in wireless networks and here we used signature detection technique to trace the intruders we also investigate a relationship between the probability of detecting an intrusion and the number of nodes that must participate in the process of detecting intrusions. Our proposal has been implemented in order to test the protocol procedure and working. 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. A Spontaneous ad-hoc network is a complete self-configured secure protocol which is able to create the network and share secure services without any previous setup. The network permits sharing resources and offering new services among users in a securely. The protocol contains all functionality required to operate without any outer support. Design of a protocol permits the creation and management of a spontaneous wireless ad hoc network

***Keywords**— public key; private key; cryptography; secure protocol; spontaneous network; wireless ad hoc networks; peer to peer network; signature based detection; intrusion detection*

I. INTRODUCTION

A. Mobile Ad Hoc Networks

With the advancement in technologies and relatively low cost, there is a rapid rise in the use of personal communication devices like mobile phones, personal digital assistants (*PDAs*) and mobile computers. These devices easily get access to network through wireless interfaces.

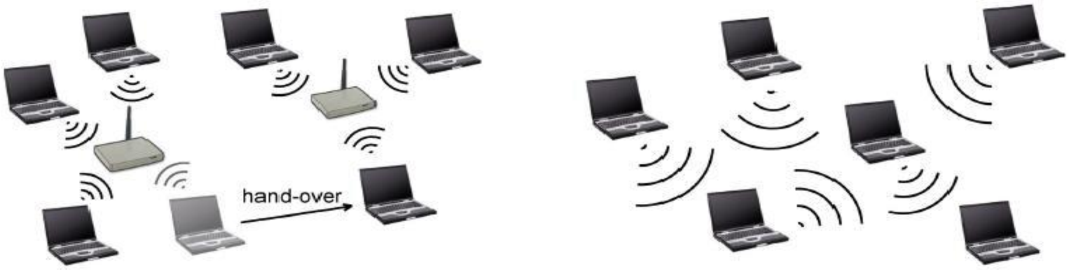

Fig 1 Infrastructured and ad-hoc networks

There exist three types of mobile wireless networks: *infrastructured networks*, *ad-hoc networks* and *hybrid networks* which combine infrastructured and ad-hoc aspects. An infrastructured network (Figure 1(a)) comprises of wireless mobile nodes and one or more connecting bridges (called as *base stations*) to connect the wireless network to the wired network. A mobile node within the network looks for the nearest base station (e.g. the one with the best signal strength), connects to it and communicates with it. In this type of network, all communication takes place between the wireless node and the base station and not between different wireless node When any mobile node gets out of range of the current base station, a *handover* to a new base station occurs and that will let the mobile node communicate seamlessly with the new base station. These wireless interfaces also allow the devices to interconnect directly with each other in a decentralized way and *self-organize* into "*Ad Hoc Networks*". An ad-hoc network does not have any infrastructure. It is devoid of base stations, routers and centralized administration. Nodes may move randomly and connect dynamically to one another. Thus all nodes act as routers and must be capable of discovering and maintaining routes to every other node in the network and to forward packets accordingly.

Mobile Ad hoc Networks (MANET) is a communication network formed by the union of autonomous aggregation of mobile nodes (computers, mobiles, PDAs etc.) and connecting wireless links. The network is modeled in the form of an arbitrary communication graph. In a MANET, there is no fixed infrastructure (Base Station) and since nodes are free to move, the network topology may dynamically change in an unpredictable manner. MANET is decentralized and self-organizing network where the functions from discovering the network topology to delivering the message are carried out by the nodes themselves; In this network each node acts as a router along with its job as an ordinary device The organization of Ad hoc networks is peer-to-peer multi hop and information packets are relayed in a store-and-forward mode from a source to any arbitrary destination via intermediate nodes. As the nodes are mobile, any change in network topology must be communicated to other nodes so that the topology information can be updated or eliminated. It is not possible for all mobile nodes to be within the range of each other. However, all the nodes are close by within radio range.

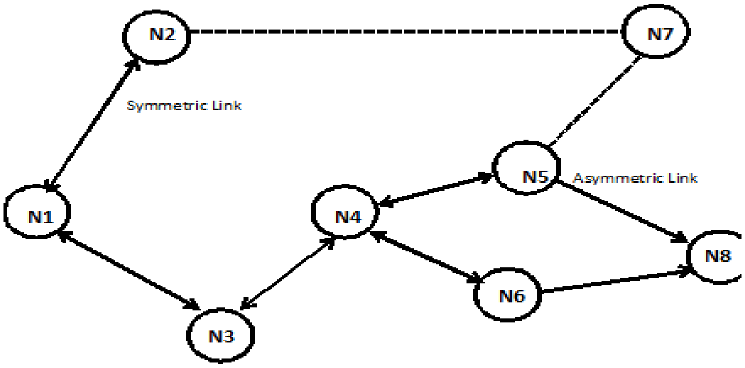

Fig 2 Mobile Ad Hoc Network Topology

B. Spontaneous Ad Hoc Networks

A spontaneous network enables the group of devices to work together and share data while they are located very close to each other with a minimum interaction. It can used to share resources and many internet services. But, we should take into account the limitation of the resources in the devices. Only once of the nodes are connected to Internet to share the connection and its resources to the all network. Moreover, configuration with the minimal interaction from the users and security over the communication should be formed. There are more application areas for ad hoc spontaneous networks: such as industrial (communication between sensor nodes, robotics, and digital networks), businesses (e.g. meeting.), and military (hard and hostile environments), and teaching. The features of spontaneous networks are as follows:

1. The network boundaries are poorly defined.
2. The network is not properly planned.
3. The hosts are not preconfigured.
4. There are not any central servers or administrator.
5. Users are not expertise.

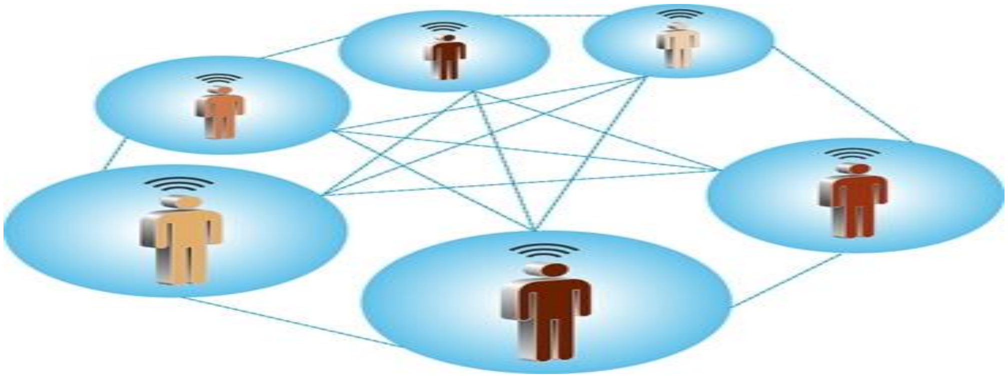

Fig 3: Spontaneous Network.

In spontaneous network there is no dependence on outside resources, people can collaborate anywhere, anything – simply and securely Mobile ad hoc network is based on human communication as shown in Figure 1. In human communication model, people come together form a group and start talking or communicating with each other by sharing their views, information and many more things. During this face to face communication anybody can talk, and join or leave the group without taking any permission. There is not any central administrator. But there is problem, if anyone leak any confidential information to other person therefore security is very important. Spontaneous networking is similar to human communication where a set of mobile nodes are placed together in a closed location for commutation to share recourses, services or computing time in limited period of time and in limited space. A set of mobile terminals that are placed in a close location communicate with each other, share the resources and services or computing time during a limited period of time and a limited space forms Spontaneous ad hoc networks. These types of networks usually have independent centralized administration. They can be wired or wireless by making Spontaneous network a Special case of ad hoc network. Spontaneous ad hoc networks need well defined, effective and userfriendly security mechanisms. Tasks to be performed in this type of network include: Identity of User, their
authorization, address to be assigned, service name, safety and operation. The Significant dependency of Configuration services in spontaneous networks is on the size of the network or nature of participates Of Nodes and running applications. Intentional interactions among users who have preferred to collaborate for some purpose is reflected by spontaneous network. It can be leveraged in order to create an ordered method for modifying the network configuration. In this type of network have limited scope in time and space. They include powerful host machines, such as laptop computers or developing high-end personal digital assistants (PDAs) and cellular phones. We present the procedures of the nodes involve in the system, the some security algorithms implementation, and the design of the messages. Moreover, we can also include the analytical proposal and its comparison with the most similar protocols in the survey. The validation of the secure protocol is carried out through several simulations and compare with regular architectures.

Intrusion detection system (IDS) plays a very important role for detecting different types of attacks. The main function of intrusion detection is to protect the network, analyze and find out intrusions among audit and normal audit data, and this can be considered as a classification problem. Intrusion detection system can be classified based on detection method into two basic methods misuse detection and anomaly detection methods. The misuse detection method operates on database of known attack signatures; the system stores patterns (or signatures) of known attacks and uses them to compare with the actual actions or activity. Another process to intrusion detection is called anomaly-based intrusion detection. Anomaly detection works on the assumption that "attack behavior" differs and distinct a sufficient amount from "normal user behavior". The Anomaly detection algorithms have the advantage over a signature-based detection that they can detect novel attacks. Although Anomaly detections methods are able to detect new types of intrusions, most of these anomaly-based IDSs suffer from a high rate of false alarms due to a deficiency in their discrimination ability.

This proposal has been develop with the main objective of improve the communication and integration between different study centers of low-resources communities. We are used by applying asymmetric cryptography, where each device have a public key and private key, key pair for device identification and symmetric cryptography is used to share session keys between nodes. Session key is referred as public key i.e. symmetric key. There are unidentified users because validity and privacy are based on user identification.

II. LITERATURE SURVEY

L.M. Feeney, B. Ahlgren, and A. Westerlund have proposed the concept of spontaneous networking in [1].

An ad hoc network work independent of any infrastructure as well as not require fixed infrastructure but for some functionality such as address allocation, name resolution, confidentiality ,service location, authentication, and access control policies, they required some administrative services. In order to solve these problems, it is necessary to leverage some aspect of the environment in which the network operates. Therefore they introduced the concept of spontaneous networking. It is created when group of people come together for some activity just like human communication model.

J. Latvakoski, D. Pakkala, and P. Paakkonen explained communication architecture concept for spontaneous network systems in [2]. 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.

The network and protocol proposed in paper [3] can established a secure self-configured environment for sharing the data and resources and services sharing among users. Security is implemented by trust network and also by increases the trust level. Consider three nodes X, Y, and Z. if X trusts Y and Y trusts Z then X will also trusts Z, by this way, trust level is implemented. Certification authority is distributed between the users that trust the new user.

In paper [3] author has 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. Also they did not consider access control and energy consumption of a node during routing of information. 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 is to be implemented in devices such as laptops, PDAs or mobile phones, with limited capacities, they must use a lightweight protocol, and new methods for control, manage, and integrate them. Methods based on imitating the behavior of human relations facilitate secure integration of services in the spontaneous networks.

In [4] Liu, J. Xu, N. Antonopoulos, J. Li, and K. Wu have proposed an Adaptive and Efficient Peer-to-peer Search (AEPS) approach for distributed service discovery for dependable service integration based on a number of social behaviour patterns, which demonstrates the following functionalities: 1. Autonomously support and co-operate with each other in a peer-to-peer (P2P) manner to quickly discover and self-configure any services available on the disaster area to deliver a real-time capability;2.Modify their behaviors to deliver a sustainable capability according to environmental changes; 3.Self-organizeitself in real time to generate higher flexibility and adaptability for disaster management systems and form groups spontaneously; [4] Share information and generate access throughout the network.

In [5] Untz, M. Heusse, F. Rousseau, and A. Duda have designed and implemented Lilith, a prototype of an interconnection node for spontaneous edge networks. It uses MPLS (Multi-Protocol Label Switching), the standard layer 2.5 for efficient forwarding of packets over various links. A flow follows a Label Switched Path (LSP) established on demand by an ad hoc routing protocol. Flows with different QoS requirements may use different LSP paths, for example time-sensitive flows such as video go over high capacity links whereas Web traffic can use other links with lower capacity, or paths are constructed over links with good radio channel quality. While the best path (in the sense of some metrics) is used at a given instant, Lilith searches for other possible paths to use in case of a link failure or a change in topology. A Lilith node expects to periodically receive messages with statistics of the traffic on each LSP received by all its immediate
neighbours. Such information can then be used to decide if a given link is broken, in which case it switches to another path. If it is not the case, Lilith uses the information to estimate link quality, the metrics that can be injected into the routing protocol.

In [6] L.M. Feeney, B.Ahlgren, A. Westerlund, and A. Dunkels have described Spontnet, a prototype implementation of a simple ad hoc network configuration utility based on basic idea of spontaneous network, much of the necessary infrastructure can be derived from the face-to-face human interactions that these networks are intended to facilitate. Spontnetallows users to distribute a group session key without previous shared context and to establish shared namespace. Two applications, a simple web server and a shared whiteboard, are provided as examples of collaborative applications that could be useful in a spontaneous networking environment. They use IPSecprotocol (used for Virtual Private Networks), applied though internet. Spontnet uses both wired and wireless links and corresponding protocols.

In [7] M. Danzeisen, T. Braun, S. Winiker, D. Rodellarhave described an implementation of a tool, which can, with the help of a cellular network, ease the formation of spontaneous networks among heterogeneous nodes.

A secure communication channel is used in the spontaneous network in order to secure the exchanged information from possible threats. This secured channelcan also be used to exchange the needed security parameters between the users, so that the future communication channel between them can be encrypted and thus protected. In the case of Bluetooth this is a PIN code, for example, and in the case of WLAN a Wired Equivalent Privacy (WEP) key. In case of the GSM network this is achieved using the Subscriber Identity Module (SIM). In future more pro-active behaviour is considered, where alternative data channels are managed continuously throughout the whole communication session allowing a dynamic handover if needed.WEP is vulnerable to hacking attacks, and better solutions, e.g., WPA, WPA2 should be considered instead. Rekimoto introduced the concept
of synchronous user operation

In [8], it described a user interface SyncTap methods for spontaneously creating network connections between the digital devices. This method can deal with multiple overlapping connection requests by detecting “collision” situations, and can also ensure secure network communication by exchanging public key information upon establishing a connection. Shared session key for secure communication is created by piggybackingDiffie-Hellman public keys (generated by each device) on multicast packets. These public keys are used to calculate a shared secret session key for encrypted communication. In this case, the authors do not propose any secure protocol. They have just added an existing security mechanism in their authentication phase. R. Lacuesta and L. Pen˜ aver have proposed work related to IP address configuration while joining a network in [9].In networking a host or node need to be configured with an IP address for communication, IP address is nothing butan identity of node in a network like name of a human being is an identity of that particular person. Generally it is given by central server but in spontaneous networking there is no central server so IP address configuration and network management is done by nodes themselves.

In [9], authors deal with the problematic of IP addresses configuration in a spontaneous network. R. Lacuesta, J. Lloret, M. Garcia, and L. Pen˜alver have developed spontaneous ad hoc network providing detail of design and simulation for the first time in [10]. They have developed protocol for spontaneous network. Also, provide security to the network. They have provided steps to be followed while joining the network. For security they have provided various security mechanisms in [10].They has also given protocol procedures and messages to be followed to transfer data. They provide mechanism to share www access service as shown in Figure 2. In this paper authors have created both analytical and simulation model and compare them with other models

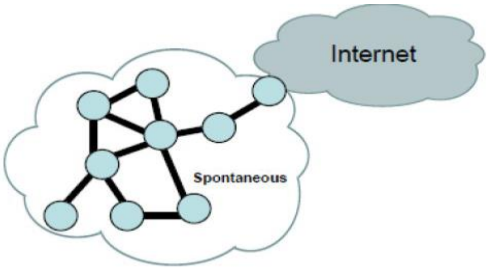

Fig 4. Spontaneous Network to share WWW access

Author R. Lacuesta in [11], has proposed architecture for security in spontaneous network in 2003.The have provided the basis to set up secure spontaneous network. R. Lacuesta, J. Lloret, M. Garcia, and L. Pen˜ alver have presented a paper that describes a security protocol for routing purposes, based on trust.

In [12], it shows two secure spontaneous wireless adhoc network protocols for wireless mesh clients that are based on the computational costs: the weak and the strong one. They are based on the trust of the users and guarantee a secure protocol between the users and the mesh routers. Both protocols provide node authenticity, intermediate node authenticity, integrity checking, random checking, verification distribution and erroneous packets elimination (before they arrive to the destination). The protocol procedure, its messages and development are explained in detail in this paper. Authors compared protocols energy consumption with other secure protocols. 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 .

Reference [14] considers specific mechanisms to detect a small set of attacks in wireless networks. The approach followed to identify the misbehaving nodes by having limits on the information that should be given out by a node in a given period of time. If a node violates this limit, then such a node is characterized as a malicious node. The approach given in this paper depends on cooperation amongst the various nodes.

III. PROTOCOL WORKING

This protocol helps to create secure spontaneous network which will be in decentralize and distributed in nature with use of different devices .cooperation between the devices allows for group service, communication, security. Spontaneous network will be created in following way

1. Node joining
2. Service Accessing
3. Trust Chain

A. *Node joining*

The joining procedure depends on the IDC i.e. Identity card which is holds by every node whether it is in network or not. The IDC contain public and private component public component is nothing but the unique name, photograph, public key, creation, and expiration time, IP. In private component contain private key which will be used for issuing certificate to valid user. When any node supposes B wants to join existing network, it must choose the node which is in communication range to validate itself (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) [4]. 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 services, data and other nodes certificates by a route involving other nodes in network. Once the node is validated then session key which is randomly created by first node of network is then distributed to all nodes of network.

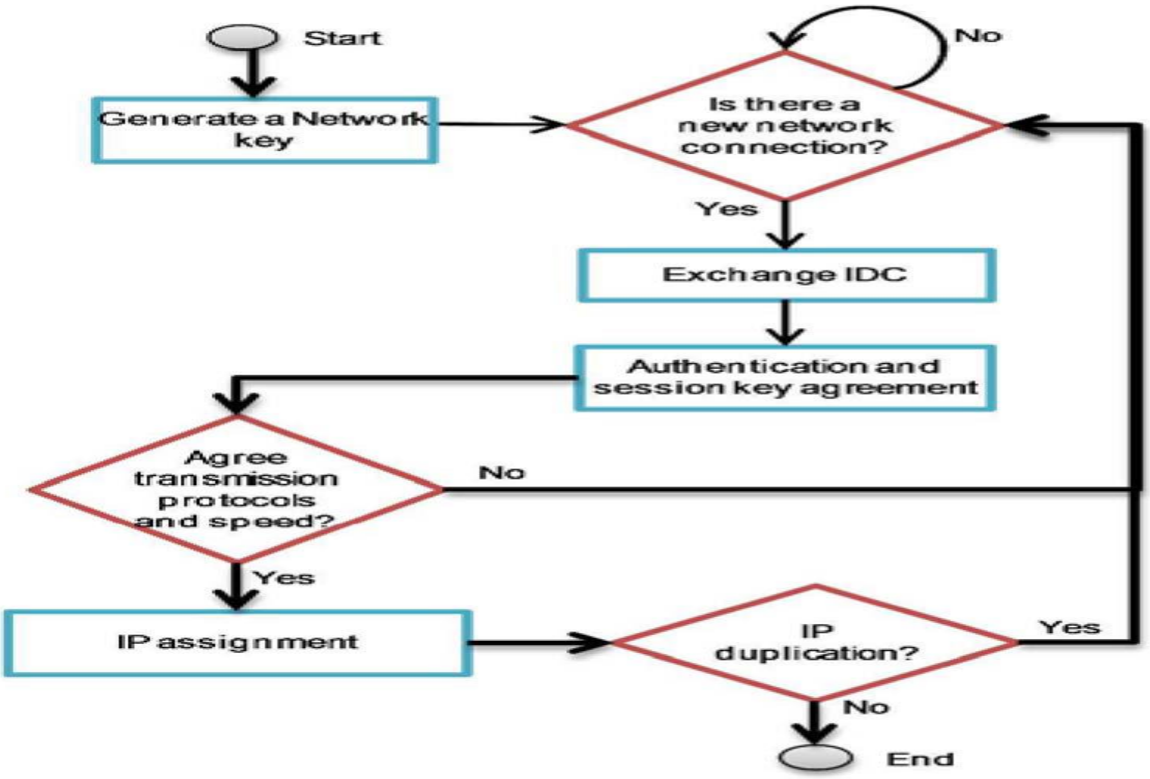
Start
Generate a Network key
Is there a new network connection?
No
Yes
Exchange IDC
Authentication and session key agreement
Agree transmission protocols and speed?
No
Yes
IP assignment
IP duplication?
Yes
No
End

Fig. 5 Joinig the new node

The node joinig procedure is combination of symmetric and asymetric key combination process in following way.Here symmetric key is use as session key to encrypt the confidential message for that Advance Encryption standard (AES) algorithm is ase . AES require less execution time and low energy consumption wheres asymmetric key cryptography is use for user authentication and session key distribution process so hence Rivest, Shamir and Adleman cryptoghraphy algorithm(RSA) is use for asymmetric key cryptoghraphy .finally IP pf new node with be generated and will check for duplication.The first node in the network will be responsible for setting the global settings of the spontaneous network (SSID, session key). However, each node must configure its own data (including the first node): IP, data, port, and user data. This information will help the node to become part of the network. After this data are saving in the first node, it changes to standby mode [5], [8]. The second node first configures its user data and security. Then, the greeting process starts. It authenticates with the first node. Our protocol relies on a sub layer protocol. The connection is created through a short-range link technology, to provide selection of nodes and ease of detection, and visual contact with the user of the node. Moreover, minimal involvement of the user is required to configure the device mainly to establish trust. This technology also borders the scope and the consumption of involved nodes. Each new node authenticates with any node in the network [7].

B. *Service Accessing*

For accessing the service the nodes in network have the agreement with each other .A user can ask other devices in order to know available services. Services have large numbers of parameter which are not transparent to user and required to configure manually. To manage the automatic integration tasks of network nodes, for example, service agents. Other is to manage secure access to the services offered by the nodes in the network. The fault tolerance is based on the routing protocol used to send information between users. Services provided by A are available only if there is a path to A, if the path to node is disappear the service is also automatically gets disappear [3]. Each node requests the services from all the other nodes that it trusts or knows nodes in the network this varies according to types of service. A request to multiple nodes is made through diffusion processes. The protocol prioritizes access to information. When the information cannot be obtained through these nodes, it can then ask other nodes. Nodes can also send requests to update network information. The reply will contain the identity cards of all nodes in the network. The nodes replying to this request sign this data ensuring the authenticity of the shipment. If it is a trusted node then its validity is also ensured, since trusted nodes have been responsible for validating their previous certificates. Under this network, any type of service or application can be implemented securely

C. *Trust Chain*

There are only two trust levels in the system, either trust or does not trust. Node A either trusts or does not trust another node B. The user interface of application installed in the device asks B to trust A when it receives the validated IDC from A. Trust relationship can be asymmetric. If node A did not establish trust level with node B directly, it can be established through trusted chains network, e.g., if A node trusts C node and C node trusts B node, then A node may trust B node. 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 [1], [10].

IV. AUTHENTICATION PROCEDURE

The authentication process for new device B is shown in Fig. 2. The receiver node A validates the received data and sends a broadcast message to B to check if these data are not used in the network (like the IP address). This IP address checking packet is sent randomly two times in order to avoid simultaneous checks and reach all devices [9], [5]. When the authentication device receives the IP checking packet, it sends the authentication reply to the new device. If any step is wrong, an error message is sent to the new device when the node is authenticated, it is able to perform several network operation and configuration task some of them are transparent to user [3].

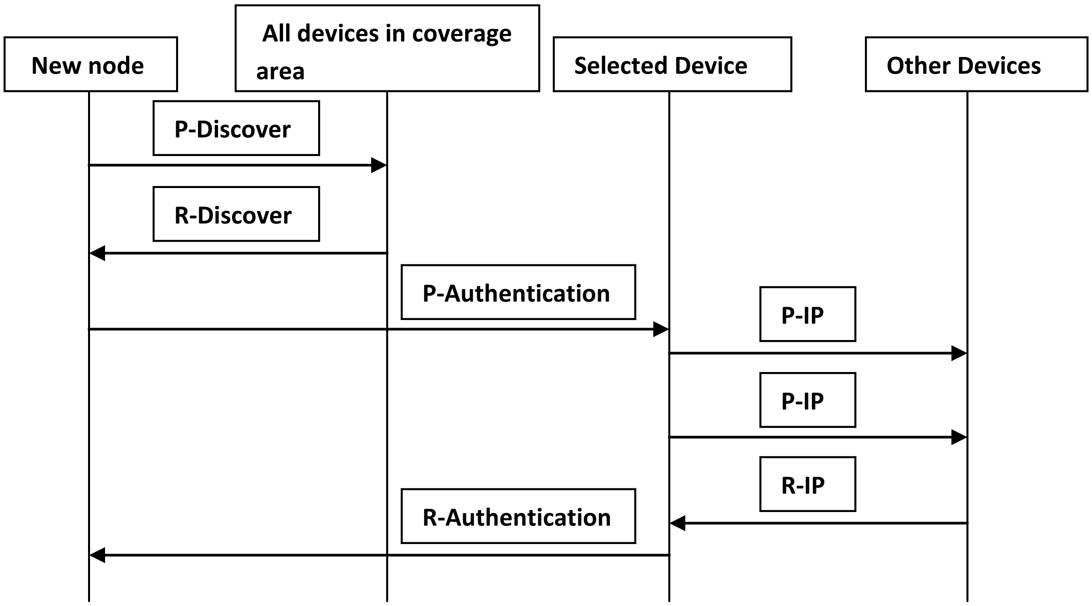

Fig. 6 Authentication Procedure

V. SESSION KEY REVOKATION

The spontaneous network is usually established for a limited period of time, which is usually not for longer time .The user certificate has an expiration time. After expiration time, the user must authenticate with the device in network. Otherwise, the device will block. Session key has an expiration time, so session key should revoke periodically. A node that leaves the spontaneous network will keep the session key until it expires. It will let the user return to the network if it has joined previously. However, if a node is disconnected from the network when the session key has been renewed, it will not be able to become the part of network until it is authenticated again with someone node from the network. The session key is formed by three parts: session key creation date/time (Fc), session key initial expiration time/date (Fe1), and the session key (Ks). The lifetime of the session key is Til = Fe1 - Fc. When a node receives the session key, it will regenerate the expiration time/date of the key by using the session key initial expiration date/ time. The expiration time/date(Fe2) is the session key initial expiration time/date plus a random number that ranges from 1 minute to the maximum anticipated duration time of the spontaneous network (this value depends on the type of spontaneous network: teaching , meeting). Fc, Fe1, Fe2, and Ks are saved in each node. Session keys do not expire at a time in all nodes. This avoids network flooding initiated at a time by many nodes, when the session key is to be revoked. When node that detects expiring session key lifetime, it will send a broadcast its current time to advise other nodes that a new session key will be generated. If to node has same session key in such case the node with oldest time wins. Once the node generate session key then, node broadcast session key encrypted with the old session key to all their neighbors. Then, the receiver will save the new session key with the new initial expiration time and will replace the old session key with the new one, thus it will only be able to communicate with only updated nodes.

VI. EVALUATION OF THE PROPOSED SCHEME

In this section we can analyze and evaluated the proposed security scheme in the spontaneous network. In proposed scheme used various types of cryptographic algorithm for secure joining of node in the new network or existing network. Following table shows the attacks in the spontaneous network and our proposal how protect against the attack.

TABLE :1
Security evaluation of Our Proposal

Attacks	**How our proposal** **Protect against attack**
Access to private user delivered data using passive spoofing	By using Symmetric encryption for guarantee for provide confidentiality
Access unreliable data	Data access only through trusted nodes
Data Modification	Hash function provide the data integrity
Network data access	Ciphered using the session key.

VII. PROTOCOL VALIDATION

Fig .7 Average delivery delay

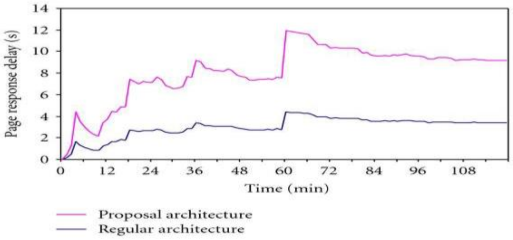

Fig .4 shows the average delivery delay it can be seen that, once the networks converge, the average delivery delay is around 9 seconds in the regular architecture and 3.5 seconds in the proposed spontaneous

VIII. INTRUSION DETECTION SCHEME

There are two types of routing protocols designed for adhoc networks, proactive routing protocols and reactive routing protocols. The proactive routing protocols attempt to maintain routing information from a given node to every other node in the network regardless of the use or need for such routes. Further, in order that the information be consistent and up-to-date, it is updated regularly irrespective of whether there is a need to send any messages on the route or not. Protocols belonging to this family require each node to maintain a set of tables to store routing information. The protocols in this family generally use distance vector shortestpath routing. A node in the system transmits its routing table periodically (time-driven updates) and also when a significant change occurs in the routing table (event-driven updates). Amongst the protocols that we consider DSDV is a proactive routing protocol.

The reactive routing protocols take a lazy approach to routing. The routes to a destination are created only when desired by a source node that desires to send data to a destination. The source node initiates the route discovery process that terminates once a route is found. Once a route has been established, it is maintained by a route maintenance procedure until either the destination becomes inaccessible or until the route is no longer desired. AODV, TORA and DSR are all reactive routing protocols. In this *intrusion detection subsystem*. We assume that there is one intruder sending a sequence of consecutive packets constituting an attack to the destination. These packets are sent in a flow consisting of normal packets. Note that the intruder is considered to be the only source of packets in all the scenarios considered in this paper. Further, we assume that the nodes that are part of the intrusion detection subsystem know this sequence of packets that constitute the intrusion. The intrusion is considered detected if this subsequence of attack packets pass through any of the nodes that constitute the intrusion detection subsystem.
So given an ad-hoc network with N nodes and a given attack signature, we use 5 different topologies (each with N nodes) and consider a sequence of five consecutive packets as constituting the attack signature. For each topology we use 3 distinct trials with each trial containing a different sequence of 5 packets that constitute the attack. In each trial we consider the intrusion detected if *all the packets that constitute the attack pass through the same node*. For a given topology the possibility of detecting an intrusion is taken to be the average over three trials. Further, for a given number of N nodes the probability of detecting an intrusion is assumed to be the averaged value over the 5 different topologies. Thus, we determine the probability of detecting an intrusion for a given number N of nodes.

We consider the dynamic case network using AODV. We assume that the intruder is moving at a speed of 15m/s. Further, we assume that the source moves such that the direction of movement in each trial is different from others. In such a case we again assume that the intrusion is detected if the packets constituting the attack pass through any node in the initial path. Here less than half the attacks are detected even for very small networks and no
attacks can be detected in large networks.

IX. CONCLUSION

Our main objective is to enable secured spontaneous networking in a user friendly way. For the initial configuration and security parameter exchange we chose to make use of a symmetric and asymmetric key cryptography, which helped us to cope with the major issues of spontaneous networking. We show the process of protocol that allows the creation and management of a spontaneous wireless ad hoc network. It imitates behavior of human relationships. It is based on a social network .Thus; each user will work to maintain the network, provide information to other network users and improve the services offered. We have proposed some procedures for self-configuration: like assigning unique IP address to each device, managing DNS and the accessing the services automatically. It is also provide the more security to data sharing with intrusion detection.

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. 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 AddressesConfiguration in Spontaneous Networks,” *Proc. NinthWSEAS 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 ProcessingSystem 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.

[13] M. Mukesh and K.R. Rishi, “Security Aspects in Mobile Ad Hoc Network (MANETs): Technical Review,” *Int’l J. Computer Applications*, vol. 12, no. 2, pp. 37-43, Dec. 2010.

[14] S. Marti, T.J. Giuli, K. Lai and M. Baker, “Mitigating Routing Misbehavior in Mobile Ad Hoc Networks”, Mobicom 2000.

[15] Y. Zhang and W. Lee, “Intrusion Detection in Wireless Ad Hoc Networks”, Mobicom 2000