ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

Volume 3, Special Issue 3, March 2014

2014 International Conference on Innovations in Engineering and Technology (ICIET'14)

On 21st& 22nd March Organized by

K.L.N. College of Engineering, Madurai, Tamil Nadu, India

Privacy Aware Protocol for Spontaneous Ad hoc Network

Elakkiya.M, CatherinJenifer.SAnandhaKumar.M.

Dept of Computer & Communication Engineering, M.A.M College of Engineering, Tamilnadu, India.

M.A.M College of Engineering, Tamilnadu, India.

Dept of Information &Technology Engineering, M.A.M College of Engineering, Tamilnadu, India.

Abstract-Ad-hoc network must operate independent of a pre-established or centralized network management infrastructure, providing administrative services needed to support applications. Address allocation, name resolution, service location, authentication, and access control policies represent some of the functionalities that support without reconfiguration or centralized services. In order to solve these problems the notion of spontaneous network is created for some collaborative activity among the group of peoples involved. A secure protocol is presented for spontaneous wireless ad hoc network and uses a hybrid symmetric/asymmetric scheme to exchange the initial data and secret keys are used to encrypt the data in the network. The Boneh and Mykletun protocols are complete self-configured to create the network and share secure services without any infrastructure. The Protocol includes all functions needed to operate without any external support. Network creation stages explains the communication, network management and protocol messages .The Boneh and Mykletun protocols are implemented to test the working procedure, performance of the network and for the secure data transmission.

Keywords- Preconfiguration, Collaborative, Boneh, Mykletun

I.INTRODUCTION

The exponential development in the development and acceptance of mobile communications in latest years is especially discerned in the fields of wireless localized systems, wireless schemes, and ubiquitous computing. This growth is mostly due to the mobility offered to users, supplying access to data any place, user friendliness, and easy deployment. Furthermore, the scalability and flexibility of wireless communications increase users' productivity and effectiveness. Spontaneous publicity hoc systems are formed by a set of mobile terminals put in a close position that broadcast with each other, distributing assets, services or computing time throughout a limited time span of time and in a restricted space, following human interaction pattern. Persons are attached to a group of persons for a while, and then depart. Network administration should be clear to the client. A spontaneous network is a special case of publicity hoc networks. They usually have little or no dependence on a centralized management. Spontaneous networks can be wired or wireless. We consider only wireless spontaneous systems in this paper. Their target is the integration of services and apparatus in the identical environment, endowing the user to have instant service without any external infrastructure. Because these systems are applied in devices such as laptops, PDAs or wireless phones, with restricted capabilities, they must use a lightweight protocol, and new procedures to command, manage, and integrate them. Configuration services in spontaneous networks count significantly on network size, the environment of the taking part nodes and running submissions. Spontaneous systems imitate human relatives while having adaptability to new condition and obvious error tolerance (the failure of a device or service should not damage the functionality). Methods based on imitating the behavior of human relatives facilitate protected integration of services in spontaneous systems. Furthermore, collaboration amidst the nodes and value of service for all shared network services should be supplied. Spontaneous publicity hoc systems need well characterized, efficient and user-friendly security means. Tasks to be presented encompass: user identification, their authorization, address allotment, title service, operation, and safety. Generally, wireless systems with infrastructure use credentials administration (CA) servers to organize node authentication and believe. These schemes have been utilized in wireless publicity hoc and sensor systems, they

are not functional because a CA node has to be online (or is an external node) all the time. Moreover, CA node should have higher computing capability.

Security should be founded on the needed confidentiality, node collaboration, anonymity, and privacy.Moreover, all nodes may not be adept to execute routing and/or security protocols, power constraints, node variability, mistake rate, and bandwidth limitations mandate conceive and the use of adaptive routing and security mechanisms, for any type of apparatus and scenarios. Dynamic networks with flexible memberships, group signatures, and distributed signatures are tough to organize. To achieve a dependable communication and node authorization in wireless ad hoc systems, key exchange mechanisms for node authorization and client authentication are required. The associated literature displays some security procedures such as pre-distribution key algorithms, symmetric and asymmetric algorithms, intermediate node-based procedures, and hybrid methods. But these methods are not enough for spontaneous networks because they need primary configuration (i.e., network configuration) or external administration (for example, centered certification administration).

The network and protocol suggested in this paper can set up a protected self-configured environment for data distribution and resources and services sharing amidst users. Security is established founded on the service needed by the users, by building a believe network to get a distributed certification authority. A user is adept to connect the network because he/she knows somebody that pertains to it. Thus, the certification authority is distributed between the users that believe the new user. The network administration is furthermore circulated, which allows the network to have a circulated name service. We apply asymmetric cryptography, where each apparatus has a public-private key two for apparatus identification and symmetric cryptography to exchange meeting keys between nodes. There are no anonymous users, because confidentiality and validity are based on client identification.

II. RELATED WORK

Latvakoski et al. interpret a connection architecture concept for spontaneous schemes, integrating application-level spontaneous assembly connection, and ad hoc networking simultaneously. A set of procedures to enable plug and play, speaking to and mobility, gaze to gaze connectivity, and the use of services are also provided. Liu et al. display how networked nodes can autonomously support and help with each other in a peer-to-peer (P2P) kind to quickly discover and self-configure any services accessible on the disaster area and deliver a real-time capability by self-organizing themselves in spontaneous groups to provide higher flexibility and adaptability for disaster monitoring and respite. Gallo et al. chased two goals in spontaneous networks: to maximize responsiveness granted some constraints on the energy cost and to minimize the energy cost granted certain obligations on the responsiveness.

Backstrom and Nadjm-Tehrani evolved the first genuine spontaneous network that boasts services dynamically utilizing the Jini expertise. They interpret the architectural conceive of the communicate service and its implementation. The prototype demonstrates how foremost conceive criteria, flexibility, dependability, efficiency, and transparency, sway conceive and services of a dynamic network of apparatus. Untz et al. suggest a lightweight and effective interconnection protocol apt for spontaneous brim networks. They conceive and apply Lilith, a prototype of an interconnection node for spontaneous brim networks. It benefits MPLS and permits different communication routes on a per flow cornerstone, supplies seamless switching between operational and back-up routes, and makes accessible information on place visited reachability. Feeney et al. offered Spontnet, a prototype implementation of a easy ad hoc network configuration utility founded on the major concepts of spontaneous networks. Spontnet allows users (using face-to-face authentication and short-range link with effortlessly identifiable endpoints) to circulate a group session key without preceding shared context and to set up distributed namespace. Two submissions, an easy World Wide Web server and a distributed whiteboard, are provided as demonstrations of collaborative applications. They use IPSec protocol (used for Virtual personal Networks), applied though internet. Spotnet therefore benefits both connected and wireless links and corresponding protocols.

Danzeisen et al. apply WEP, the normal security means utilized in Wireless LANs, available by default in the IEEE 802.11 wireless protocol. Other suggestions that did not discuss security aspects could furthermore request this default solution. whereas it was accessible to us, we did not use it because WEP is vulnerable to hacking attacks, and better solutions, e.g., WPA, WPA2 should be advised rather than. Rekimoto introduced the notion of synchronous user procedure and recounted a user interface SyncTap technique for spontaneously setting up network connections between digital apparatus. This procedure can deal with multiple overlapping attachment requests by noticing “collision” situations, and can also ensure protected network communication by swapping public key information upon setting up a connection. Distributed session key for protected communication is conceived by piggybacking Diffie-Hellman public keys (generated by each apparatus) on multicast packets. These public keys are utilized to assess a distributed secret meeting key for encrypted communication. In this case, the authors do not propose any protected protocol. They have just added an existing security means in their authentication stage. It is similar to the one utilized by us when a new node joins our network, but we have supplemented other security means in alignment to create a complete secure protocol for spontaneous systems. Spontaneous systems are also exceptional case of human centric networks Cornelius et al. applied and assessed Anony Sense, a general-purpose structure for anonymous opportunistic tasking and reporting, which allows applications to query and obtain context through an expressive task dialect and by leveraging a very wide variety of sensor types on users’ wireless devices, and at the same time respects the privacy of the users.

III.SECURE SPONTANEOUS NETWORK

A. NETWORK OVERVIEW

Our protocol permits the creation and administration of distributed and decentralized spontaneous systems with little intervention from the user, and the integration of different apparatus (PDAs, cell phones, laptops, etc.). Cooperation between apparatus allows provision and access to distinct services, such as assembly communication, collaboration in program delivery, security, etc. The network members and services may alter because apparatus arefreetojoin or leave the network. Spontaneous network should entire the following steps in alignment in which they are created.

1) Step1: Connecting Procedure: This step endows apparatus to communicate, including the self-acting configuration of ordered and personal parameters. The system is based on the use of the personal business card (IDC) and a certificate. The IDC contains public and personal components. The public constituent comprises of ordered Identity (LID), which is exclusive for each client and allows nodes to identify it. It may encompass data such as title, image or other kind of client identification. This concept has been utilized in other systems such as in vehicular ad hoc networks. It furthermore comprises the user's public key

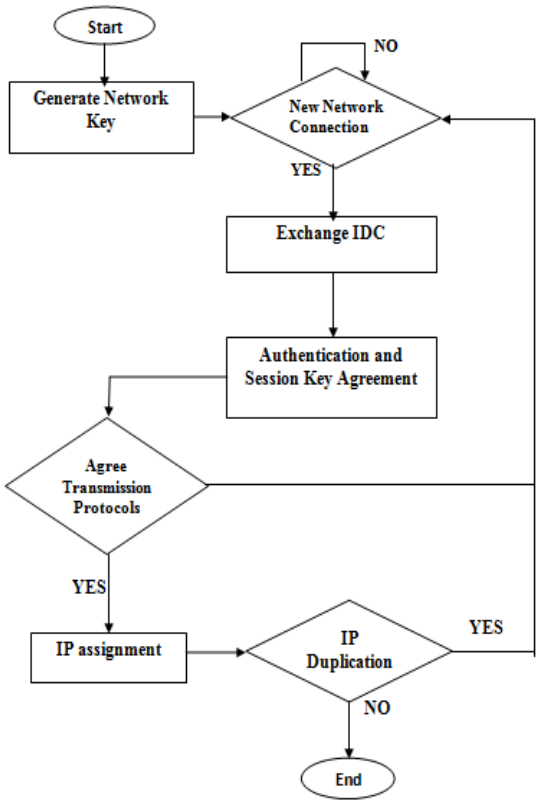

Fig1. Algorithm for Joining New node.

(Ki), the creation and expiration designated days, an IP proposed by the user, and the client signature. The client signature is developed utilizing the Secure Hash Algorithm (SHA-1) on the previous data to get the data abstract. Then, the data abstract is marked with the user's personal key. The personalconstituent comprises the personal key (ki). The client inserts its individual data (LID) the first time he/she uses the scheme because the security data is generated then.

Security facts and figures are retained persistently in the apparatus for future use. Certificate Cij of the client i comprises of a validated IDC, marked by a client j that presents its validity. To get IDC signature of user the abstract function got by SHA- 1 is marked with j's personal key. No centered certification administration is used to validate IDC. Validation of integrity and authentication is finished mechanically in each node. The certification administration for a node could be any of the trusted nodes. This scheme endows us to construct a circulated certification authority between trusted nodes. When node A wants to communicate with another node B and it does not have the certificate for B, it demands it from its trusted nodes. After getting credentials of the system will validate the facts and figures; if it is correct then it will signal this node as a legitimate node. All nodes can be both clients and assistrs, can request or assist demands for information or authentication from other nodes. The first node conceives the spontaneous network and develops a random meeting key, which will be swapped with new nodes after the authentication stage. The stages of a node joining the network: node authentication and authorization, affirmation on meeting key, transmission protocol and speed, and IP address and routing. When node B likes to connect an existing network, it should select a node within communication range to authenticate with (e.g., node A). A will drive its public key. Then, B will drive its IDC signed by A's public key. Next, A validates the received facts and figures and verifies the hash of the message in order to check that the data has not been modified. In this step, A sets up the believe grade of B by looking physically at B (they are physically close), counting on whether A knows B or not. Eventually, A will send its IDC facts and figures to B (it may do so even if it concludes not to trust B). These facts and figures will be marked by B's public key (which has been received on B's IDC). B will validate A's IDC and will set up the trust and validity in A only by integrity verification and authentication. If A does not answer to the connecting request, B should choose another network node (if one exists).

After the authentication, B can access facts and figures, services, and other nodes certificates by a path engaging other nodes in network. Security administration in the network is founded on the Public Key Infrastructure and the symmetric key encryption design. Symmetric key is utilized as a session key to cipher the confidential messages between trusted nodes. It has less power requirements than the asymmetric key. We have utilized the sophisticated Encryption benchmark (AES) algorithm for the symmetric encryption design. It offers high security because its design structure removes sub key symmetry. Furthermore execution times and energy utilization in cryptography methods are adequate for low-power apparatus.

The asymmetric key encryption design is used for circulation of the meeting key and for the client authentication process. We utilized two kinds of

asymmetric encryption designs: Elliptic Curve Cryptosystem (ECC), because of its high performance and the Rivest, Shamir &Adleman cryptographic algorithm (RSA). After the mutual authentication, A will encrypt the session key with B's public key and will drive it to B. Then, they will acquiesce the transmission protocols and the wireless attachment speed. Eventually, B will configure IP address and routing B develops a data. IP address which has a repaired part in the first two bytes and the rest is formed by a random number which depends on the user's facts and figures. Then, B will drive the data to process the routing data to A. A will check whether the IP is replicated in the network. When B sends data to other network nodes, for example, node C, these data will be validated by C (using hashing and authentication methods). Afterwards, C will set up the trust grade with B, by looking bodily. If no believe level is established, it will be done after by utilizing trusted chains in the network.

2.) Step2: Services Discovery: B asks for the accessible services. Services can be found out utilizing Web Services recount dialect (WSDL). Our model is based on but in our spontaneous network we don't use a centered server. Moreover, other service discovery services can be applied in our scheme client can inquire other devices in order to know the accessible services. It has an affirmation to allow get access to its services and to get access to the services suggested by other nodes.

Services have a large number of parameters which are not clear to the client and require manual configuration. One topic is to organize the self-acting integration jobs and use, for demonstration, service agencies. Other is to manage protected get access to the services suggested by the nodes in the network. The obvious error tolerance of the network is based on the routing protocol utilized to send data between users. Services provided by B are accessible only if there is a route to B, and go away when B leaves the network.

3.)Step 3: Establishing Trust chains and changing Trust Level: There are only two believe grades in the scheme. Node A either believes or does not believe another node. The software e submission established in the device inquires B to trust A when obtains the validated IDC from B. Trust connection can be asymmetric. If node A did not establish believe grade with node B directly, it can be established through trusted chains, for example, if A trusts C and C believes B, then A may believe B. believe level can change over time depending on the node's demeanor. Therefore, node A may conclude not to trust node B although A still trusts C and C trusts B. It can also halt believing if it discovers that preceding trust string of links does not exist anymore.

B. PROTOCOL AND NETWORK ADMINISTRATION

In the network formation, nodes perform the primary exchange of configuration data and security using the means of authentication or welcome based on the other works. This mechanism avoids the need for a central server, making the jobs of building the network and adding new members very easy. The network is conceived utilizing the information supplied by users, therefore, each node is identified by an IP address. Services are shared utilizing TCP attachments. The network is constructed utilizing IEEE 802.11b/g expertise which has high data rates to share assets. We have booked the short-range technology (Bluetooth) to permit authentication of nodes when they connect the network.

After the authentication method, each node learns the identity business card of other renowned nodes, a public key and a top. This data will be revised and completed all through the network nodes. This structure supplies an authenticated service that verifies the integrity of the data from each node because there is a distributed CA. Each node demands the services from all the nodes that it trusts, or from all known nodes in the network, counting on the kind of service. A request to multiple nodes is made through diffusion processes. The protocol prioritizes get access to data through trusted nodes. When the data will not be obtained through these nodes, it can then inquire other nodes. Nodes can furthermore drive requests to revise network data. The answer will comprise the persona cards of all nodes in the network. The node answering to this request should signal these facts and figures ensuring the authenticity of the shipment. If it is a trusted node, its validity is also double-checked, since trusted nodes have been responsible for validating their preceding credentials. Under this network, any kind of service or application can be applied. The services suggested by our protocol will be protected.

C. NETWORK CREATION

The first node in the network will be responsible for setting the international settings of the spontaneous network (SSID, meeting key), each node must configure its own facts and figures (including the first node): IP, port, facts and figures security, and client facts and figures. This information will permit the node to become part of the network. After this data are set in the first node, it alterations to standby mode.

D. CONNECTING NEW MEMBERS

The second node first configures its user facts and figures and network security. Then, the greeting method begins. It authenticates against the first node. Our protocol relies on a sub layer protocol (which can be Bluetooth or Zigbee). The connection is created through a short-range connection expertise, to provide flexibility and ease of detection and assortment of nodes, and visual communicate with the client of the node. Furthermore, minimal engagement of the user is needed to configure the device, mostly to set up believe. This expertise also bounds the scope and the consumption of engaged nodes. Each additional node authenticates with any node in the network.

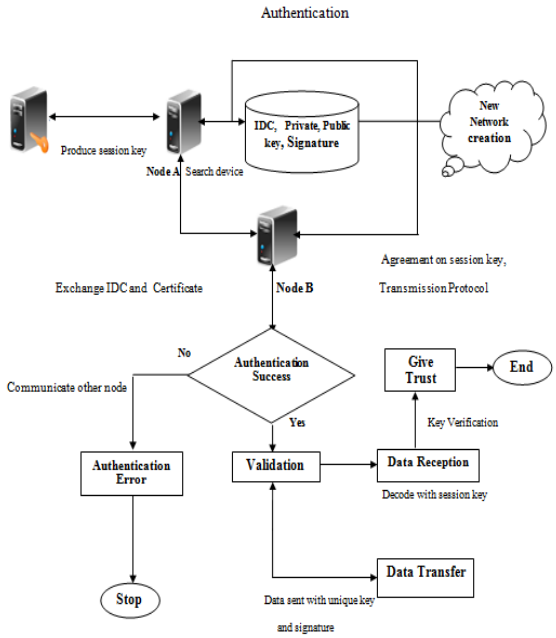

Fig2. SystemArchitecture.

In alignment to conceive the design drawings of the protocol, we have used the Unified Modeling dialect (UML). The UML is a visual specification normalized dialect that is built to model object oriented schemes. We use keys, undertakings, and use cases (diagrams offered by the benchmark) to define the processes, the structure of the categories in the scheme, and the behavior of things or procedures. One time validation/registration method of the user in the apparatus has been done, he/she should determine if to create a new network or take part in an existing one. If he/she decides to conceive a new network, it begins with the following method.

First, a session key will be developed. Then, the node will start its services (including the network and authentication services). Eventually, it will wait for demands from other apparatus that want to join the network. If the client wants to become part of the living network, the node pursues algorithm to find a apparatus that will give trust to it, save corresponding facts and figures and will adept to begin communications. The node that pertains to the network, and is responsible for validating the new node's facts and figures, will perform a diffusion method to the nodes that are inside its communication range. These nodes will ahead the obtained packets to their neighbors until the facts and figures reach all nodes in the network. This process permits verifying the validity and uniqueness of the new node's data. The authentication process for new device B is shown. The receiver node A validates the obtained facts and figures and drives a announced message to B to ascertain if these facts and figures are not utilized in the network (even the IP address). This IP ascertaining packet is sent randomly two times in alignment to bypass simultaneous tests and come to all apparatus. When the authentication apparatus receives the IP checking answer, it sends the authentication answer to the new apparatus. If any step is wrong, a mistake note is dispatched to the new device. When the node is authenticated, it is adept to present some tasks. Some of them are presented clearly for the client, but other ones are utilized by the client to present some operations in the network. They are the user application choices. Fig. 4 shows the structure of the programmed application in UML dialect. The authenticated node can present the following jobs:

- Display the number of nodes.
- Change the trust of nodes.
- Revise the information: It permits a node to discover about other nodes in the network and also to drive its facts and figures to the network. This revise could be for only one client or for all clients in the network through a controlled diffusion process.
- Other nodes certificate request: A node could be demanded from other node, from all trusted nodes or from all renowned nodes. In case of all renowned nodes, the node that replies to the request will habitually sign the facts and figures. The facts and figures will be considered validated if a trusted node has signed them. Authentication demand: The node authenticates a requesting node by validating the obtained information, user authentication, and verifying the non duplication of the top facts and figures and the proposed IP.
- Answer to a data request: the demanded data will be dispatched directly to the requesting node or routed if the node is not on the connection range.
- Data demand: The demand will be forwarded if it is a announced message.
- Drive data to one node: It can be dispatched symmetrically or asymmetrically encrypted, or unencrypted. Send data to all nodes: This method is doing by a flooding scheme. Each node retransmits the facts and figures only the first it obtains the facts and figures. It can be sent symmetrically encrypted or unencrypted.

E.SESSION KEY

Session key has an expiration time, so it is revoked periodically. A node that departs the spontaneous network will keep the meeting keys until it expires. It will let the user come back to the network if it has connected before (the spontaneous network is generally set up for a restricted period of time, which is generally not very long). If a node is disconnected from the network during the period of time when the meeting key has been improved, it will not be able to get access to the network until it is authenticated afresh with somebody from the network. The session key is formed by three areas meeting key creation time/date (Fc), session key primary expiration time/ designated day (Fe1), and the meeting key (Ks). When a node receives the session key, it will redevelop the expiration time/date of the key by using the session key initial expiration time/ date. The expiration time/date Fe2 is the meeting key initial expiration time/date plus a random worth that varieties from 1 minute to the greatest anticipated length time of the spontaneous network Fc, Fe1, Fe2, and Ks are retained in each node. Meeting keys do not expire simultaneously in all nodes. It avoids network flooding

(to announce about the need for new session key) started simultaneously by many nodes, when the session key is to be revoked. Node that detects expiring session key lifetime will drive an announced note (with its present time) to suggest other nodes that a new meeting key will be generated, and to bypass duplications (in the event of a tie, the node with oldest time wins). Then, the node sending the announced note will generate the new meeting key and will announced it encrypted with the vintage session key to all their neighbors, to be eavesdropped). Then, the receiver will shop the new meeting key with the new meeting key initial expiration time and will replace the old session key with the newone.

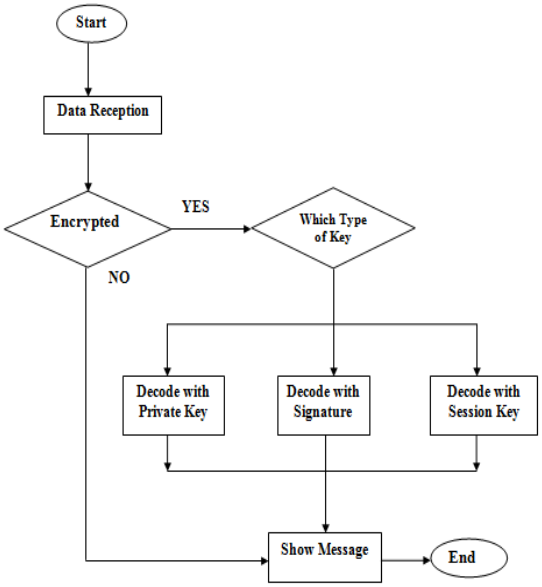

Fig3. Algorithm for ReceivingData.

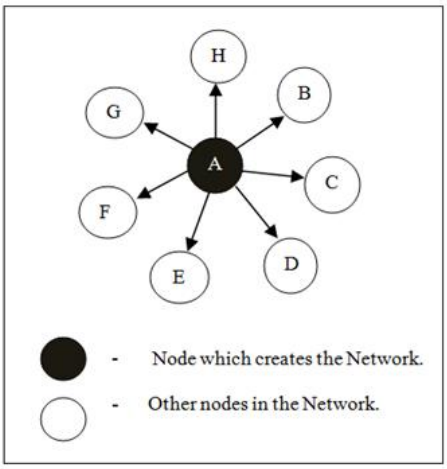

Fig4. Spontaneous Network.

F. SECURE DATA TRANSMISSION IN SPONTANEOUS NETWORK

After all the authentication and identification process in the spontaneous network nodes transfer data with nearest trustable nodes. The user can ask other devices in order to know the available services. It has an agreement to allow access to its services and to access the services offered by other nodes. Services provided by a node are available only if there is a path to that node, and disappear when the node leaves the network. After that node can send data to another node by symmetrically encrypted and the receiver checks whether it is encrypted or not and decode with session key or private key. So the receiver check the data and update the regarding information such as trust level, integrity etc. This process is done by using Boneh and Mykletun which is a key and signature based Encryption schemes. The following Table Ishow the security evaluation of our proposal in which our proposal refuses theattacksoccurring in this proposed system.

Table II explains the comparison of Spontaneous network with other networks with their Intervention, self configuration, security, prototype and their programming languages.

TABLE I: Security Evaluation of Our Proposal

Attacks	How our Proposal Refuse the attacks
Access to Use Data in physical data	User/ Password Access.
Compromised Physical Device	User/ Password Access, Visual Identity Verification (Authentication Phase).
Identity Impersonation	Trust Policies, Visual Identity Verification (Authentication Phase).
Phishing, active spoofing, compromised data	Hashing and authentication. Use of Trusted chain.
Data access using passive spoofing.	Ciphered using session key, Key management.
Access to private user delivered data using passive spoofing	Asymmetric or symmetric encryption guaranteeing confidentiality.
Data modification	Hash function to guarantee data integrity.
Data transmission	Signature based Encryption.

TABLE II: Comparison of Spontaneous Network

S.NO	PURPOSE	Need for user Intervention	Self Configuration	Security	Real Prototype	Programming Language
1	Learning Environment	Medium	Yes	No	No	-
2	Contact Service	Low/Medium	Yes	No	Yes	JAVA
3	Interconnection edge Networks	Low	Yes	No	Yes	-
4	Simple web server and a shared white Board	Low	Yes	Yes (IPsec)	Yes	-
5	Cellular Networks	Low	Yes	Yes(WEP)	No	-
6	Exchange of Data	Low/Medium	Yes	Yes (Diffie-Hellman)	Yes	-
Our Proposal	Resource Sharing	Low	Yes	Yes(Complete Security Protocol)	Yes	JAVA

ACKNOWLEDGEMENT

I would like to express my special thanks of gratitude toMr.ShenbagarajanAnantharajan, Mr.SibiChakkaravarthy as well as our guide Mr.Anantha Kumar who helped me in completing my work. Secondly I would like to thank my parents, my friends and well wishers who were a constant source of Inspiration.

CONCLUSION

In this paper, we display the design of a protocol that permits the creation and administration of a spontaneous wireless adhoc network. It is founded on a social network imitating the demeanor of human connections. Therefore each user will work to sustain the network, advance the services suggested, and supply data to other network users. We have supplied some methods for self-configuration: A unique IP address is assigned to

each apparatus, the DNS can be organized efficiently and the services can be found out automatically. We have furthermore conceived a user-friendly submission that has negligible interaction with the client. A user without advanced mechanical information can set up and participate in a spontaneous network. The security designs included in the protocol allow protected communication between end users (bearing in mind the resource, processing, and power limitations of publicity hoc devices). We have presented some checks to validate the protocol operation. They showed us the advantages of using this self-configuring ad hoc spontaneous network. The answer times got are apt for use in real environments, even when apparatus have limited resources.

Storage and volatile recollection desires are rather reduced and the protocol can be utilized in normal resource-constrained apparatus (cell phones, PDAs...). We intend to add some new characteristics to the client submission (such as distributing other kinds of resources, etc.) and to the protocol, such as an intrusion detection mechanism and a circulated Domain Name Service by utilizing the LID and IP of the nodes and uses secure protocol for data transmission. Now, we are working on supplementing other types of nodes that are adept to share their services in the spontaneous network. The new nodes will not count on a user, but on an entity such as a shop, a bistro, or other kinds of services.

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. Lloret, L. Shu, R. Lacuesta, and M. Chen, *"User-Oriented and Service-Oriented Spontaneous AdHoc and Sensor Wireless Networks,"* Ad Hoc and Sensor Wireless Networks, vol. 14, nos. 1/ 2, pp. 1-8, 2012.

[3] S. Preuß and C.H. Cap, *"Overview of Spontaneous Networking - Evolving Concepts and Technologies,"*RostockerInformatik-Berichte, vol. 24, pp. 113-123, 2000.

[4] R. Lacuesta, J. Lloret, M. Garcia, and L. Penalver, *"A Spontaneous Ad-Hoc Network to Share WWW Access,"* EURASIP J. Wireless Standards and Technology," http://www.itl.nist.gov/fipspubs/Comm. and Networking, vol.2010, article 18, 2010.

[5] Y. Xiao, V.K. Rayi, B. Sun, X. Du, F. Hu, and M. Galloway, "A [27] A. Wander, N. Gura, H. Eberle, V. Gupta, and S. Chang, *"Energy Survey of Key Management Schemes in Wireless Sensor Net-works"*
Computer Comm.vol. 30, nos. 11/12, pp. 2314-2341, Sept. 2007.

[6] V. Kumar and M.L. Das, *"Securing Wireless Sensor Networks [28]* N.R. Potlapally, S. Ravi, A. Raghunathan, and N.K. Jha, *"Analyze- with Public Key Techniques,"* Ad Hoc and Sensor Wireless Networks, vol. 5, nos. 3/4, pp. 189-201, 2008.

[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, pp. 567-585, Sept. 2006.

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

[9] 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.

[10] 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, pp. 37-43, Dec. 2010.

[11] 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, pp. 122-140, 2011.

[12] 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.

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

[14] R. Lacuesta and L. Penalver,˜*"Automatic Configuration of Ad-Hoc Networks: Establishing Unique IP Link-Local Addresses,"* Proc. Int'l Conf. Emerging Security Information, Systems and Technologies (SECURWARE '07), 2007.

[15] 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.

[16] 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.

[17] S. Gallo, L. Galluccio, G. Morabito, and S. Palazzo, *"Rapid and Energy Efficient Neighbor Discovery for Spontaneous Networks,*"Proc. Seventh ACM Int'l Symp.
Modeling, Analysis and Simulation of Wireless and Mobile Systems, Oct. 2004.

[18] J. Backstrom and S. Nadjm-Tehrani, *"Design of a Contact Service in a Jini-Based Spontaneous Network,"* Proc. Int'l Conf. and Exhibits on the Convergence of IT and Comm., Aug. 2001.

[19] 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.

[20] 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.