Volume 3, Issue 11, November 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Spontaneous Wireless Ad Hoc Networking: A Review

Prof.D.N.Rewadkar
Associate Professor, Computer Engineering, RMD Sinhgad School of Engineering, Pune University, India

Smita Karve
M.E. Research Scholar, Computer Engineering, RMD Sinhgad School of Engineering, Pune University, India

Abstract— Communication in wireless network is based on client server model where an infrastructure is required between two clients or mobile to communicate with each other even though they are closed to each other. In human communication model, two people those are physically closed to each other can talk directly without any server. In spontaneous network there is no server or any infrastructure between nodes to communicate, anybody those who wants to communicate can join, communicate and leave the network without any central server. It is based on peer to peer network, where nodes can join and leave network and share or distribute information to each other like human communication model. As spontaneous network is self configured a security is a major concern. So a secure self configured protocol is required for user authentication, validation and data transfer. 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. Secured protocol uses a hybrid symmetric/asymmetric key encryption scheme for user authentication and to exchange data. It is self configured as it is used to create and manage network, also manage resource sharing and providing services without any central infrastructure. In this paper, we study all work to be done on spontaneous network and various security mechanisms to be provided.

Keywords— Spontaneous network, cryptography, MANET, secure protocol, peer-to-peer network

I. INTRODUCTION

Mobile Ad hoc network (MANET) is a group of wireless nodes that form a network without support of any kind of infrastructure. Following are features of MANET:

- Host movement frequent
- Topology change frequent
- No cellular infrastructure.
- Multi-hop wireless links.
- Data must be routed via intermediate nodes

Though MANET is a good option over infrastructure dependent network, it has some challenges. They are, first, the network must operate independent of an access point infrastructure, even though the connectivity among nodes changes rapidly and unpredictably. Second, the network must operate independent of a preestablished or centralized network management infrastructure, while still providing administrative services to support applications. And third, routing in MANET is done by some routing protocol like DSR, DSDV or AODV. To achieve a reliable communication and node authorization in mobile ad hoc networks, key exchange mechanisms for node authorization and user authentication are needed security methods such as pre-distribution key algorithms, symmetric and asymmetric algorithms, intermediate node based methods, and hybrid methods. Spontaneous networking is solution to these problems of MANET which 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, join or leave the group without taking any permission. There is not any central coordinator. But the problem is, if somebody 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. They usually have little or no dependence on a centralized administration. Spontaneous network can be wired or wireless. We only consider wireless spontaneous network for our review in this article. In spontaneous network ad hoc network new services are added without user intervention. Failure or breakdown of any attached service or device does not compromise functionality of network. Network boundaries are poorly defined. The network is not planned. Hosts are not preconfigured. There are not any central servers. Users are not experts. All these are features of spontaneous network. Spontaneous adhoc network is a special case of Mobile Ad hoc network (MANET). A major problem in mobile ad hoc networks is the management and dissemination of information. Since the mobile devices are restricted in their resources, a complete replication of information will not be possible. Information exchange should be restricted with respect to the spatial scope of the information and the interests of the user. Another issue is the multitude of available information: how can a user determine or specify which information is interesting to him or her? Solution to these problems is Spontaneous adhoc network. These networks are implemented in

devices such as laptops, PDAs or mobile phones with limited space and time. As we all know, Personal digital assistants (PDAs) and cell phones become universal data terminals; sensors and actuators in home and industry automation are controlled via digital networks; the TV set evolves to a control terminal for air conditioning and lighting.

Figure 1: Spontaneous Networking. Because there is no dependence on outside resources, people can collaborate anywhere, anything – simply and securely

The amount of networked devices currently runs towards infinity. In the same way grows the administration effort for handling this amount. Common techniques of manual parameter configuration and software installation do not satisfy the needs for more mobility, dynamic and user friendliness. The currently evolving methods for spontaneous networking of devices and services could be one way out of this situation. In a plug and play manner they can minimize the effort to integrate devices and services into network environments. In these networks node can join or leave the network in an adhoc manner it might be vulnerable to attack if nodes are not trusted. Therefore security is a major concern while designing and developing spontaneous adhoc network in mobile devices. 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.

Security in networks must involve authentication, confidentiality, node cooperation, anonymity, and privacy also. To transfer photo require less security but to transfer confidential information require high security therefore encryption and decryption techniques are required to share information. In wireless ad hoc networks Certificate Authority (CA) is used to authenticate the user and manage the trust. For this CA requires high computing capacity and time and also it has to be online. In such networks, for node authorization and user authentication a dependable media is required and there may be single point of failure. Security in spontaneous is based on the users service needs, and to obtain a distributed certification authority it necessary to build trust networks. The network allows users to join because it belongs to someone who knows it. Hence, the new user is trusted by the certification authority. This allows the network to have a distributed name service and also distribution of network management.

II. STUDY OF EXISTING SYSTEM

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 but for some functionality such as address allocation, name resolution, 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.Therfore they introduced the concept of spontaneous networking. It is created when group of people come together for some activity just like human communication model. They have explained five challenges of spontaneous network [1]:

1. Network boundaries are poorly defined.
2. The network is not planned.
3. Hosts are not preconfigured.
4. There are not any central servers.
5. Users are not experts

J. Latvakoski, D. Pakkala, and P. Paakkonen explained communication architecture concept for spontaneous 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. A set of methods to enable plug and play, addressing and mobility, peer to peer connectivity and use of services are also provided.

The network and protocol proposed in paper [3] can establish a secure self-configured environment for data distribution and resources and services sharing among users. Security is implemented by trust network and also by increasing level of trust. Consider three nodes A, B, and C. if A trusts B and B trusts C then A will also trusts C, 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 are implemented in devices such as laptops, PDAs or mobile phones, with limited capacities, they must use a lightweight protocol, and new methods to control, manage, and integrate them. 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.

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:

- 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;
- modify their behaviors to deliver a sustainable capability according to environmental changes;
- self-organize themselves in real time to generate higher flexibility and adaptability for disaster management systems and form groups spontaneously;
- Share information and generate access throughout the network.

AEPS has no single point of failure, ensuring greater dependability and availability. AEPS is able to efficiently discover desirable services for decision making of disaster monitoring and relief by interacting with connected nodes with incomplete information and to support dependable dynamic service integration through coping with rapid and significant changes in the disaster area. AEPS builds a "social" network for each sensor node which contributes to effective service discovery. 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. Spontnet allows 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 IPSec protocol (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. Rodellar have 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 channel can 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. The needed authentication is provided implicitly by the cellular operator. 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. Furthermore, inbound signalling over an established data link will improve the performance of the system. In that case the usage of the cellular would be limited to the bootstrapping phase and as fallback signalling channel. 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], and described a user interface SyncTap technique for spontaneously establishing network connections between 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 piggybacking Diffie-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 but

an 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.

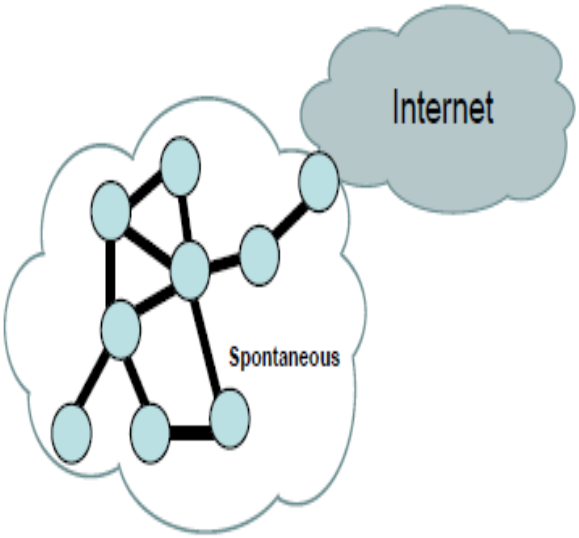

Figure 2. Spontaneous Network to share WWW access

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 ad-hoc 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 [13], [14].

In order to study security aspects we study paper [13], in which various security aspects in MANET are given. Impacts of various security attacks on new protocol in MANET are explained in detail in [14].And mechanism of Bluetooth has been studied in [15]. C. Cornelius, A. Kapadia, D. Kotz, D. Peebles, M. Shin, and N. Triandopoulos have described AnonySense, a privacy-aware architecture for realizing pervasive applications based on collaborative, opportunistic sensing by personal mobile devices in [16]. AnonySense allows applications to submit sensing tasks that will be distributed across anonymous participating mobile devices, later receiving verified, yet anonymized, sensor data reports back from the field, thus providing the first secure implementation of this participatory sensing model. They also described a trust model, and the security properties that drove the design of the AnonySense system. This paper does not tackle routing issues in spontaneous ad hoc wireless networks. A paper that presents a security protocol for routing purposes, based on trust, is shown in [12] as explained above.

III. CONCLUSION

In this paper we have studied work related to spontaneous wireless ad hoc network along with technologies required to build and secure the network. As it is a social kind of network work as peer to peer network nodes are themselves responsible for all network activities like creating network, joining new node, providing services and so on. They have provided a unique IP address to each node of the network for its identity. Also provide trust of chain to authorize the new user. For s communication they have used either gateway or Bluetooth technologies. We also study various security majors have been taken to secure the network. Security has been provided by various cryptographic encryption/decryption techniques. We have discussed all these technologies with their advantages and disadvantages in detail. We study there are two major things that are creating and managing network and protocol design. A lot of work has been done but still we can add some new features to the user application (such as sharing other types of resources,

etc.) and to the protocol, such as an intrusion detection mechanism and a distributed Domain Name Service by using the LID and IP of the nodes. Also we can add Access control list over shared resources so that we can more secure our network from unauthorized access.

REFERENCES

[1]. L.M. Feeney, B. Ahlgren, and A. Westerlund, "Spontaneous Networking: An Application-Oriented Approach to Ad-hocNetworking," *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 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.

[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] 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.

[15]. R. Lacuesta and L. Herrero, "A Good Use of Bluetooth, A Good Use of Bluetooth," *Proc. Int'l Workshop Advanced Web Eng. for e- Business (AWEEB '04)*, Mar. 21, 2004.

[16]. C. Cornelius, A. Kapadia, D. Kotz, D. Peebles, M. Shin, and N. Triandopoulos, "Anonysense: Privacy-Aware People-Centric Sensing," *Proc. Sixth Int'l Conf. Mobile Systems, Applications, and Services (MobiSys '08)*, pp. 17-20, June 2008.

