International Journal of Research
Available at https://edupediapublications.org/journals

p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 17
November2016

A New Approach Using Secure Public Key Techniques Without Group Manager For Spontaneous Wireless Networks

[1]D. Sanjeeva Kumar, [2] K. Janardhan

[1]*M.Tech, Dept of CSE, Intell Engineering College,Anantapuramu,Affiliated to JNTUA, AP, India*
[2] *Associate Professor , Dept of CSE Intell Engineering College,Anantapuramu,Affiliated to JNTUA, AP, India*

Abstract: *This paper presents a secure protocol for spontaneous wireless unexpected networks that uses Associate in Nursing hybrid symmetric asymmetric theme and therefore the trust between users so as to exchange the initial knowledge and to exchange the key keys that may be used to cipher the information. Trust relies on the primary visual contact between users. Our proposal may be a complete self-configured secure protocol that is able to produce the network and share secure services with none infrastructure. The network permits sharing resources and offering new services among users in a very secure setting. The protocol includes all functions required to work with none external support. We've designed and developed it in devices with restricted resources. Network creation stages area unit elaborated and therefore the communication, protocol messages, and network management area unit explained. Our proposal has been enforced so as to check the protocol procedure and performance. Finally, we tend to compare the protocol with alternative spontaneous unexpected network protocols so as to highlight its options and that we offer a security analysis of the system.*

I. INTRODUCTION

The exponential growth within the development and acceptance of mobile communications in recent years is especially discovered within the fields of wireless native space networks, mobile systems, and present computing. This growth is principally as a result of the quality offered to users, providing access to data anyplace, user friendliness, and easy readying. Moreover, the measurability and flexibility of mobile communications increase users' productivity and potency. Spontaneous impromptu networks are shaped by a group of mobile terminals placed in a very shut location that communicate with one another, sharing resources, services or computing time throughout a restricted amount of your time and in a very limited area, following human interaction pattern. People are hooked up to a gaggle of individuals for a jiffy, and then leave. Network management ought to be clear to the user. A spontaneous network could be a special case of impromptu networks. They sometimes have very little or no dependence on a centralized administration. Spontaneous networks are often wired or wireless. we tend to contemplate solely wireless spontaneous networks during this paper. Their objective is that the integration of services and devices within the same atmosphere, sanctioning the user to possess instant service with none external infrastructure. Because these networks are enforced in devices like laptops, PDAs or mobile phones, with limited capacities, they have to use a light-weight protocol, and new ways to manage, manage, and integrate them. Configuration services in spontaneous networks rely significantly on network size, the character of the collaborating nodes and running applications. Spontaneous networks imitate human relations whereas having ability to new conditions and fault tolerance (the failure of a tool or service shouldn't injury the functionality). Ways based mostly on imitating the behavior of human relations facilitate secure integration of services in spontaneous networks. Moreover, cooperation among the nodes and quality of service for all shared network services ought to be provided. Spontaneous impromptu networks need well outlined, efficient and easy 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. Though these systems are used in wireless impromptu and detector networks, they are not sensible as a result of a CA node needs to be on-line (or is associate external node) all the time. Moreover, CA node should have higher computing capability. Security ought to be supported the desired confidentiality, node cooperation, anonymity, and privacy. Exchanging photos between friends needs less security than exchanging confidential documents between enterprise managers. Moreover, all nodes might not be ready to execute routing and or security protocols. Energy constraints, node variability, error rate, and information measure limitations mandate the design and use of adaptative routing and security mechanisms, for any sort of devices and eventualities. Dynamic networks with versatile memberships, group signatures, and distributed signatures are troublesome to manage. To attain a reliable communication and node authorization in mobile impromptu networks, key exchange mechanisms for node authorization and user authentication are needed. The connected literature shows many security ways such as pre distribution key algorithms, parallel and asymmetric algorithms, intermediate node-based ways, and hybrid ways. However these ways aren't enough for spontaneous networks as a result of they have associate initial configuration (i.e., network configuration) or external authorities (for example, central certification authorities). None of the prevailing papers propose a secure spontaneous network protocol supported user trust that gives node legitimacy, integrity checking, and privacy. The network and protocol planned during this paper will establish a secure self-configured atmosphere for information distribution and resources and services sharing among users. Security is established supported the service needed by the users, by building a trust network to get a distributed certification authority. A user is in a position to affix the network as a result of he/she knows somebody that belongs thereto. Thus, the certification authority is distributed between the users that trust the new user. The network management is additionally distributed, which allows the network to possess a distributed name service. We apply uneven cryptography, wherever every device encompasses a public-private key combine for device identification and parallel cryptography to exchange session keys between nodes. There are not any anonymous users, as a result of confidentiality and validity are supported user identification.

2. RELATED WORK

In [15], Latvakoski et al. make a case for a communication design concept for spontaneous systems, integration application-level spontaneous cluster communication, and ad hoc networking along. a collection of ways to alter plug and play, addressing and quality, peer to look connectivity, and also the use of services also are provided. Liu et al.

II. show however networked nodes will autonomously support and get together with one another during a peer-to peer (P2P) manner to quickly discover and self-configure any services on the market on the area and deliver a real-time capability by self-organizing themselves in spontaneous groups to supply higher flexibility and adaptableness for disaster observance and relief. Gallo et al.

pursued 2 targets in spontaneous networks: to maximize responsiveness given some constraints on the energy value and to attenuate the energy value given bound necessities on the responsiveness. Nadjm-Tehrani [18] developed the primary real spontaneous network that gives services dynamically using the Jini technology. They make a case for the field of study design of the contact service and its implementation. The prototype demonstrates however major standard, flexibility, dependability efficiency, and transparency, affect the design and services of a dynamic network of devices. In [19], Untz et al. propose a light-weight and economical interconnection protocol appropriate for spontaneous edge networks. They style and implement Lilith, an image of associate degree interconnection node for spontaneous edge networks. It uses MPLS and permits totally different communication ways on a per flow basis, provides seamless change between operational and back-up ways, and makes on the market information on destination reachability. Feeney et al. [20] given Spontnet, a image implementation of a straightforward unintentional network configuration utility

supported the most ideas of spontaneous networks. Spontnet permits users (using face-to-face authentication and short-range link with simply diagnosable endpoints) to distribute a bunch session key while not previous shared context and to determine shared namespace. 2 applications, a simple internet server and a shared whiteboard, are provided as samples of cooperative applications. They use IPSec protocol (used for Virtual personal Networks), applied although net. Spotnet thus uses each wired and wireless links and corresponding protocols.

3. EXISTING SYSTEM

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 behavior 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.

DISADVANTAGES OF EXISTING SYSTEM

- All nodes may not be able to execute routing and/or security protocols. Energy constraints, node variability, error rate, and bandwidth limitations mandate the design and use of adaptive routing and security mechanisms, for any type of devices and scenarios.
- Dynamic networks with flexible memberships, group signatures, and distributed signatures are difficult to manage.
- To achieve a reliable communication and node authorization in mobile ad hoc networks, key exchange mechanisms for node authorization and user authentication are needed security methods such as pre-distribution key algorithms, symmetric and asymmetric algorithms, intermediate node-based methods, and hybrid methods.
- But these methods are not enough for spontaneous networks because they need an initial configuration or external authorities.

4. PROPOSED SYSTEM

The network and protocol proposed in this paper can establish a secure self-configured environment for data distribution and resources and services sharing among users. Security is established based on the service required by the users, by building a trust network to obtain a distributed certification authority. A user is able to join the network because he/she knows someone that belongs to it. Thus, the certification authority is distributed between the users that trust the new user. The network management is also distributed, which allows the network to have a distributed name service. We apply asymmetric cryptography, where each device has a public-private key pair for device identification and symmetric cryptography to exchange session keys between nodes. There are no anonymous users, because confidentiality and validity are based on user identification.

ADVANTAGES OF PROPOSED SYSTEM

- We presented the basis to setup a secure spontaneous network
- To solve mentioned security issues, we used an authentication phase and a trust phase
- We 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. We have used this mechanism in the secure protocol presented in this paper, but it can be replaced by any other IP address assignment mechanism.

5. SYSTEM ARCHITECTURE

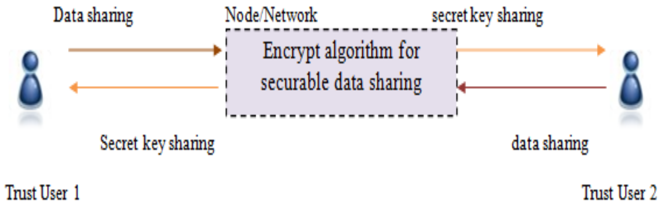

Fig 1: **Architecture diagram for Secure Protocol for Spontaneous Wireless Ad Hoc Networks Creation**

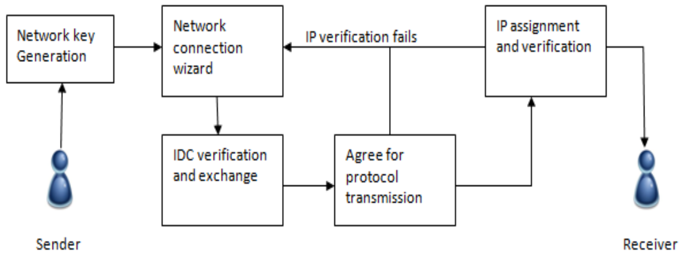
Network key Generation
Network connection wizard
IP verification fails
IP assignment and verification
IDC verification and exchange
Agree for protocol transmission
Sender
Receiver

Fig 2 Architecture diagram for New Node

6. IMPLEMENTATION

A. Network Setup Model

- ➢ The user can register and login with the owner permission whether to join new node and or an existing node or to create a network.
- ➢ The owner provides session key based on the requirements of the trusted user.

B. Trusted User and node creation Module

- ➢ In this module, the trusted user gets login by admin permission.
- ➢ The data is shared between two trusted users by session key generation for their respective data's and encrypting their files.
- ➢ The user can only access the data file with the encrypted key if the user has the privilege to access the file.

- Validation of integrity and authentication is done automatically in each node.
- And this forms a Spontaneous Wireless Ad Hoc node creation between trusted authorities (users).

C New node Joining Module

- By using Network based Intrusion Detection System (NIDS),the new node is created and they are joined to new nodes by respective procedures given by owner.
- The joining module is done with 3 phases:

(i)Joining Procedure

- After joining the node, they are provided with IDC(Identity card and Certificate). IDC Contains both public key(user's information, IP) and private key(user signature).
- The certification authority for a node could be any of the trusted nodes. This system enables us to build a distributed certification authority between trusted nodes.
- For example When node A wants to communicate with another node B and it does not have the certificate for B, it requests it from its trusted nodes. After obtaining this certificate the system will validate the data; if correct then it will sign this node as a valid node. All nodes can be both clients and servers, can request or serve requests for information or authentication from other nodes.

(ii)Services Discovery

- If a node asks for the available services. Services can be discovered using Web Services Description Language (WSDL).
- Our model is based on, but in our spontaneous network we don't use a central server. Moreover, other service discovery services can implemented in our system.

(iii) Establishing Trusted Chain and Changing Trust Level

- There are only two trust levels in the system.

For e.g., Node A either trusts or does not trust another node B. The software application installed in the device asks B to trust A when it receives the validated IDC from B.

- Trust relationship can be asymmetric.
- If node A did not establish trust level with node B directly, it can be established through trusted chains, e.g., if A trusts C and C trusts B, then A may trust B. 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.

D. New network creation module

- In this module, we create a new network for the trusted users.
- The first node in the network will be responsible for setting the global settings of the spontaneous network.
- The second node first configures its user data and network security.
- Our protocol relies on a sub layer protocol **e.g.,** Bluetooth.
- After encountering the device, the authentication request is sent to another user.
- if authentication is accepted, it asks for data exchange .If failed the device wont exchange data
- The authenticated node can perform the following tasks:

- Display the nodes.
- Modify the trust of the nodes and Update the information.
- Send data to all nodes
- Leave the network
- Process an authentication request etc., based on the a secure protocol for spontaneous wireless ad hoc

E. Data transfer module

- A node receives a data packet that is ciphered by a public key.
- When the server process received the packet, it is in charge of deciphering it with the private key of the user.

VI. CONCLUSION

In this paper, we show the design of a protocol that allows for the construction and management of a spontaneous wireless ad hoc network. It's centered on a social community imitating the conduct of human relationships. Thus, every user will work to maintain the community, give a boost to the offerings provided, and provide understanding to other network users. We've supplied some techniques for self-configuration: a unique IP address is assigned to each and every gadget, the DNS can be managed effectively and the services will also be learned automatically. Now we have also created a consumer-friendly utility that has minimal interplay with the user. A person without evolved technical capabilities can installed and participate in a spontaneous network. The safety schemes included within the protocol enable cozy conversation between finish users (bearing in intellect the useful resource, processing, and vigour obstacles of ad hoc networks). We've carried out a few tests to validate the protocol operation. They showed us the advantages of making use of this self-configuring ad hoc networks. The response instances bought are suitable to be used in actual environments, even when contraptions have limited resources. Storage and unstable memory desires are rather low and the protocol can be used in standard resource-constrained instruments (cell phones, PDAs...). We intend to add some new features to the consumer software (similar to sharing different varieties of resources, and so on.) and to the protocol, corresponding to an intrusion detection mechanism and a dispensed area name carrier by using the LID and IP of the nodes. Now, we are engaged on adding other types of nodes which might be capable to share their services within the spontaneous network. The new nodes won't depend upon a person, however on an entity comparable to a shop, a cafe, or other types of offerings.

.

References

[i] 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.

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

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

[iv] 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.

[v] Y. Xiao, V.K. Rayi, B. Sun, X. Du, F. Hu, and M. Galloway, "A Survey of Key Management Schemes in Wireless Sensor Networks," Computer Comm., vol. 30, nos. 11/12, pp. 2314-2341, Sept. 2007.

[vi] V. Kumar and M.L. Das, "Securing Wireless Sensor Networks with Public Key Techniques," Ad Hoc and Sensor Wireless Networks, vol. 5, nos. 3/4, pp. 189-201, 2008.

[vii] 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.

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

[ix] 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.

[x] 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.