A Secure Symmetric Key Protocol For on Demand Wireless Ad-hoc Networks

#Department of computer science and engineering, Mallareddy engineering college, maisamaguda, Dhulapally, Secundrabad-11

V.S.K Chaitanya¹, P.V Ramana Murthy²
M.Tech # Assistant professor #
shrikrishna@gmail.com ramanamurthy19@gmail.com

Abstract: Wireless network are becoming popular now a days due their features like easy setup without the need of cabling. Wireless ad-hoc networks are a collection of mobile/semi-mobile nodes with no pre-established infrastructure, forming a temporary network. Each node in the network has a wireless Interface and communicates with each other over either radio frequency or infrared, that is, point to point communication. In this paper a symmetric key protocol for spontaneous wireless ad hoc network creation which uses a hybrid symmetric scheme. In our proposal is 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 no need any external support for handling the functionalities of the network. A spontaneous ad hoc network is complete self configured secure protocol which is able to create the independent network and share the secure services without any setup and offer the new services among users are present in the secure environment. This protocol contains all function required to operate without any external support. Design of a protocol make available the creation and management of a spontaneous wireless ad hoc network.

I. Introduction

The computing sector has emerged as a lifeline of today’s generation. In the computing industry Wireless network has become very popular. Wireless network are used to make capable portability. Mobile networks are divided into two types, first is A network with wired and fixed entrance or we can say portal. It is also called infrastructure network. Every network should only have Root Bridge that is called base station. A mobile unit within the network connects to and communicates with the nearest base station. 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 user-friendly 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.

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. The caching technique is used to avoid the overload of the nodes. Moreover, configuration with a minimal interaction from the users and security over the communication should be formed. There are more application areas for ad hoc spontaneous networks: industrial (communication between sensor nodes, robotics, and digital networks), businesses (meeting, stock control, etc.), military (hard and hostile environments), and teaching. The range of environment in which those networks can be applied is wide and may conference services and other "ubiquitous computing" applications at home, office and etc. This paper also shows the design and
simulation of a Model that lets optimal spontaneous network access by using the caching mechanism. 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. 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 use 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. There are unidentified users because validity and privacy are based on user identification.

II. Related Work

Wireless technologies are used by millions of mobile professionals in world, many big companies to solve business problems and create merits over their contestans. HP solutions are giving legal power to mobile or remote workers to access data, knowledge, business intelligence and many other applications from various places. Mobile professionals use this new advantage to work more productively, better satisfy customers, and generate more sales. Users are finding that wireless LANs provide more flexibility to configure an office and can improve both the productivity and the collaboration of office workers. These solutions help HP customers create value for their customers and an advantage over their competitors. All of this can be accomplished in a relatively cost-effective, more secure manner. New standards based technologies offer improved methods to authenticate and better secure devices, helping ensure that only authorized user’s access networks. HP understands wireless technology and knows how to design hardware, software applications, and consulting and network management service solutions to meet business needs. The time for wireless technology has come. In telecommunications, wireless communication may be used to transfer information over short distances (a few meters as in television remote control) or long distances (thousands or millions of kilometers for radio communications). Wireless does not mean sparks, noise, or a lot of switches. Wireless means communication without the use of wires other than the antenna, the ether, and ground taking the place of wires. Radio means exactly the same thing: it is the same process. Communications by wireless waves may consist of an SOS or other messages from a ship at sea or the communication may be simply the reception of today’s top 10 music artists, or connecting to the Internet to check your email. It does not become something different in either spelling or meaning. The term is often shortened to "wireless": It encompasses various types of fixed, mobile, and portable two-way radios, cellular telephones, personal digital assistants (PDAs), and wireless networking. Other examples of wireless technology include GPS units, garage door openers and or garage doors, wireless computer mice, keyboards and headsets, satellite television and cordless telephones. The several security methods such as redistribution key algorithm, symmetric and asymmetric algorithm, and intermediate node based methods but these types of methods are not suitable for the spontaneous network creation because they need a network configuration or external authorities. Existing methods propose a secure spontaneous network protocol based on the users trust which provides node authenticity integrity checking, confidentiality. We present a basic setup of the symmetric key protocol to handle the security issues; we can use the authentication stages and trust stages. In this paper also include the intrusion detection scheme for joining the new member in the network while that node are authenticate or not. Mobile Ad-hoc Networks is a collection of two or difficult in a spontaneous wireless network, because that more nodes equipped with wireless communications and doesn’t have a fixed infrastructure. The major problem innetworking capability. These nodes can communicate ensuring security service in an MANET lies on managing with other nodes that immediately within their radio range the keys and providing privacy for data communication or outside their radio range. The Spontaneous Wireless [15]. Ad-hoc. Spontaneous wireless ad hoc networks are created Networks does not have any gateway, every node by a set of mobile terminals placed in a close location that can act as the gateway.
The notion of a mobile ad hoc communicate with other mobile terminal, sharing network is a network formed without any central resources, services or computing time during a limited administration which consists of mobile nodes that use a period of time and in a limited space wireless interface to send packet data. Since these nodes Network management should be transparent/visible in a network can act as routers and hosts, to the user. A spontaneous wireless ad hoc network is aConfidentiality, integrity and authentication are special case of wireless ad hoc networks. They usually secure features wireless ad hoc network, so these have no dependence on a centralized administration.

![Network Modal](image)

Fig1: Network Modal.

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. The caching technique is used to avoid the overload of the nodes. Moreover, configuration with a minimal interaction from the users and security over the communication should be formed. There are more application areas for ad hoc spontaneous networks: industrial (communication between sensor nodes, robotics, and digital networks), businesses (meeting, stock control, etc.), military (hard and hostile environments), and teaching. The range of environment in which those networks can be applied is wide and may conference services and other "ubiquitous computing" applications at home, office and etc. This paper also shows the design and simulation of a Model that lets optimal spontaneous network access by using the caching mechanism. 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. This proposal has been develop with the main objective of improve the communication and integration between different study centers of low-resource communities. We are use 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. There are unidentified users because validity and privacy are based on user identification.

### III. Security-Aware Ad-Hoc Routing (SAR)

Security-Aware Ad-Hoc Routing (SAR) is the generalized framework for any on-demand ad-hoc routing protocol. SAR requires that nodes having same trust level must share a secret key. SAR augments the routing process using hash digests and symmetric encryption mechanisms. The signed hash digests provide message integrity while the encryption of packets ensures their confidentiality.

**Operation** SAR when implemented on AODV protocol adds two additional fields to the Route Request packet and one additional to the Route Reply packet. The first field added to the Route Request packet is the security requirement field and is set by the sender. It indicates the preferred level of trust for the path to the destination. The Second field added to is the security guarantee that signifies the maximum level of security provided by the discovered paths. If the security requirement field has an integer representation then the security guarantee field will be minimum of all security levels of the participating nodes in the path. If the security requirement field is represented in vectors then the security guarantee field value...
is computed by ANDing the security requirement values of the participating nodes in the path. The value thus computed is copied into additional security guarantee field of the Route Reply packet and sent back to the sender. This value is also copied into the routing of nodes in the reverse path, to preserve the security information with reference to cashed paths strengthens the scheme by forbidding nodes from spoofing at the data link layer. To achieve thses goals a Neighbor Lookup Protocol (NLP) is made an integral part of SLSP. The NLP is responsible for the following tasks. Maintaining a mapping of MAC and IP layer addresses of the node’s neighbors. Identify potential discrepancies, such as the use of multiple IP addresses by a single data-link interface. Measuring the rates at which control packets are received from each neighbor by differentiating the traffic primarily based on MAC address. This rate of incoming control packets helps in discarding nodes which maliciously seek to exhaust network resources.

IV. Security in spontaneous network
Portable nodes that need to communicate to reduce time slot for the creation of spontaneous ad hoc networks. The problems of ad hoc network are similar to these networks, but they increased because they are temporal networks form in a given that moment by a group of nodes that often users don’t know each other. However, they can work together for the proper process of the network. Safe communication must be guaranteed with the help of cryptographic techniques. However, many of the outlined protocols assume that every node know the session key. When we talk about the use of cryptography of private key as well as the cryptography of public key. Methods to establish a secure and authentic communication channel is provided by these networks, assuming that the participants know the node which they are speaking with them and share the data. A fundamental topic in the security of the spontaneous networks creation, when the nodes do not know each other and also the phase of connection establishes and initial exchange of keys. Security requirements in spontaneous networks and traditional networks are same: privacy, integrity, verification, no repudiation, and availability, confidentiality. Both data as well as routing information must be safe. The structures of ad hoc networks make these necessities much more difficult: dynamic topology, limited bandwidth, different capacity links and high error rates, energy and processing capacity Limitations, no central server, and often no prior information in the nodes to build the network. These limitations have to be covered by organization mechanisms and by the support among the nodes to maintain service quality, security, and almost inventions and access to the Services and share data. Like human relationships in the society, this Behavior is also similar to them. Everyone must cooperate to preserve a secure world, to improve our quality of life, and have updated news. We know that the data should be correct when they come from a person that we trust. In this society the trust is very important. Our goal to develop technique in order to enable the creation of small-medium-scale ad hoc networks based on the spontaneity of both. On the grounds of physical proximity, wireless connectivity is based; it reflects the ways of the human beings interact. People who are near each other can link, share things with each other, and ask people relay information to other users. That is all done with an appropriate Level of security.

V. Symmantic Routing Protocol
SR is one of the most well known routing algorithms for ad hoc wireless networks. It was originally developed by Johnson, Maltz, and Broch. SR uses source routing, which allows packet routing to be loop free. It increases its efficiency by allowing nodes that are either forwarding route discovery requests or overhearing packets through promiscuous listening mode to cache the routing information for future use. SR is also on demand, which reduces the bandwidth use especially in situations where the mobility is low. It is a simple and efficient routing protocol for use in ad hoc networks. It has two important phases, route discovery and route maintenance. The main algorithm works in the following manner. A node that desires communication with another node first searches its route cache to see if it already has a route to the destination. If it does not, it then initiates a route discovery mechanism. This is done by sending a Route Request message. When the node gets this
route request message, it searches its own cache to see if it has a route to the destination. If it does not, then appends its id to the packet and forwards the packet to the next node; this continues until either a node with a route to the destination is encountered (i.e. has a route in its own cache) or the destination receives the packet. In that case, the node sends a route reply packet which has a list of all of the nodes that forwarded the packet to reach the destination. This constitutes the routing information needed by the source, which can then send its data packets to the destination using this newly discovered route. Although DSR can support relatively rapid rates of mobility, it is assumed that the mobility is not so high as to make flooding the only possible way to exchange packets between nodes.

Secret key cryptography

In secret key cryptography, a single key is used for both encryption and decryption. The sender uses the key (or some set of rules) to encrypt the plaintext and sends the ciphertext to the receiver. The receiver applies the same key to decrypt the message and recover the plaintext. Because a single key is used for both functions, secret key cryptography is also called symmetric encryption. With this form of cryptography, it is obvious that the key must be known to both the sender and the receiver; that, in fact, is the secret. The biggest difficulty with this approach, of course, is the distribution of the key [5].

Public key cryptography

Public or asymmetric key cryptography involves the use of key pairs: one private key and one public key. Both are required to encrypt and decrypt a message or transmission. The private key, not to be confused with the key utilized in private key cryptography, is just that, private. It is not to be shared with anyone. The owner of the key is responsible for securing it in such a manner that it will not be lost or compromised. On the other hand, the public key is just that, public. Public key cryptography intends for public keys to be accessible to all users. In fact, this is what makes the system strong. If a person can access anyone public key easily, usually via some form of directory service, then the two parties can communicate securely and with little effort, i.e. without a prior key distribution arrangement.

SYMMETRIC KEY ALGORITHM

Algorithm
Step 1: Generate the ASCII value of the letter
Step 2: Generate the corresponding binary value of it. [Binary value should be 8 digits e.g. for decimal 32 binary number should be 00100000]
Step 3: Reverse the 8 digit's binary number
Step 4: Take a 4 digits divisor (>=1000) as the Key
Step 5: Divide the reversed number with the divisor
Step 6: Store the remainder in first 3 digits & quotient in next 5 digits (remainder and quotient wouldn’t be more than 3 digits and 5 digits long respectively. If any of these are less than 3 and 5 digits respectively we need to add required number of 0s (zeros) in the left hand side. So, this would be the ciphertext i.e. encrypted text. Now store the remainder in first 3 digits & quotient in next 5 digits.

VI. Evolution

We can notice that there is no significant difference at both encoding method. The same files are encrypted by two methods; we can recognize that the two curves almost give the same results. The results show the superiority of Blowfish algorithm over other algorithms in terms of the processing time. Another point can be noticed here; that RC6 requires less time than all algorithms except Blowfish. A third point can be noticed here; that AES has an advantage over other 3DES, DES and RC2 in terms of time consumption and throughput. A fourth point can be noticed here; that 3DES has low performance in terms of power consumption and throughput when compared with DES. It requires always more time than DES because of its triple phase encryption characteristics. We can find in decryption that Blowfish is the better than other algorithms in throughput and power consumption. The second point should be notice here that RC6 requires less time than all algorithms except Blowfish. A third point that can be noticed is that AES has an advantage over other 3DES,DES RC2. The fourth point that can be considered is that RC2 still has low performance of these algorithm. Finally, Triple
DES (3DES) still requires more time than DES.

![Time Consumption of the Symmetric Algorithm](image)

**Fig 2.** Time Consumption of the Symmetric Algorithm.

Encryption time is used to calculate the throughput of an encryption scheme. It indicates the speed of encryption. The throughput of the encryption scheme is calculated by dividing the total plaintext in Megabytes encrypted on the total encryption time for each algorithm in. As the throughput value is increased, the power consumption of this encryption technique is decreased.

**VII. Conclusion**

the various features of wireless networks, adhoc wireless networks and the routing protocols for wireless adhoc networks. In this paper provide complete self-configured Symmetric secure protocol which is described gives more trusted way to spontaneous ad hoc network with every node maintain the network, improves the services offered, and provide information to other network node for the Formation Spontaneous ad hoc networks. The protocol allows secure communication between end users includes the security schemes, with the help of intrusion detection provide more security and share the data.

**References:**


