INTEGRATED SECURITY FRAMEWORK FOR HYBRID WIRELESS MESH NETWORKS

Paramjeet Rawat[1], Dr. M.S.Aswal[2]

[1]IIMT Engg. College, U.P., India (paramjeet.rawat@gmail.com),

[2]Vidya Engg. College, U.P.,India(mahendra8367@gmail.com)

Abstract – Hybrid Wireless Mesh Network is a special case of infrastructural mesh network which utilizes heterogeneous wireless networks for communication. The integration of WMNs with other networks such as the Internet, cellular, IEEE 802.11, IEEE 802.15, IEEE 802.16, sensor networks, etc., can be accomplished through the gateway and bridging functions in the mesh routers. An integrated security mechanism is a key challenge in the integration on such networks. In this paper, we analyze the problems in the integration of various heterogeneous wireless network's. Thereafter, we proposed a integrated security framework for the hybrid WMN which helps in building a secured environment for communication within the network. The proposed mechanism efficiently uses the characteristics of WMN's, mutual authentication and secretes key cryptography to provide a integrated security for heterogeneous wireless mesh networks.

Keywords – Hybrid wireless mesh networks, security, cryptography, heterogeneous wireless network.

I. *INTRODUCTION*

Wireless mesh networks (WMNs) have emerged as a key technology for next-generation wireless networking. A **wireless mesh network** (**WMN**)[1] is a communications network made up of radio nodes organized in a mesh topology. There are two types of nodes in WMNs: mesh routers and mesh clients. All of the nodes in WMNs are considered as a host and a router. They leave the data which are forwarded to themselves and transmit the data which are for others. Therefore, the data will be kept forwarding until they arrive at the destination. Compared with traditional wireless networks, such as ad hoc networks, WMNs have the following main features: first, the mesh routers are relatively stationary, hence, the routing paths can be created that are likely to be stable; second, all traffic is either to or from a designated gateway which connects the WMNs to the Internet; third, the power consumption of the mesh routers is not significant.

WMN has gained considerable attention in recent years not only due to its fast deployment, easy maintenance and low upfront investment compared with traditional wireless networks, but also its support of the existing wireless networks, such as wireless sensor networks, wireless fidelity network (Wi-Fi), and so on. Such a type of network is termed as hybrid mesh network. From the user's perspective, the future networks will implement supporting ubiquitous and consistent access to the networks and preserving the user interfaces to network services, independent of the location of the user, including when the user roams across different networks.

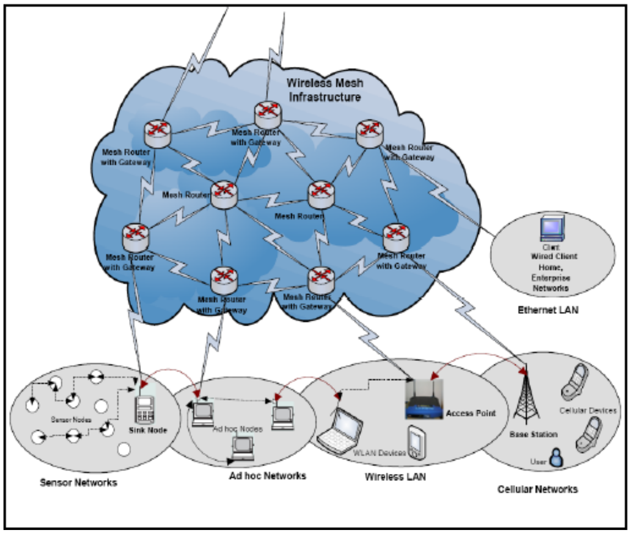

Figure1: Heterogeneous Network Integration Model

This realization of the future network will be accomplished through the integration of the various different wireless networks. To integrate several wireless networks into a single architecture, there are a number of challenges that must be addressed; these include support for mobility management, quality of service (QoS) provisioning, and security interoperability. Especially, integration of security techniques used by these various and different networks is one of the key problems, as due to the inherent vulnerability of wireless communications, the security requirements of wireless communication are usually more stringent than in wired networks. Also, because of the inherent and often quite fundamental differences among the various wireless networks, integration of the security schemes of those networks is not an easy task.

In the following section, we discuss some of those differences.[2]

- **Architectural characteristics**: Basic characteristics, such as device capacity, radio bandwidth, coverage area, maximal transmission power, and other architectural features can significantly differ among various wireless networks.
- **Security requirements**: The security requirements of network communication services are tailored to the special requirements of the applications and the capabilities of a network. The implementation of those security requirements must match the available network services.
- **Selected security mechanisms and standards**: The designers of each network adopted a particular set of security mechanisms and standards, which in general, may not be compatible with those of the other related wireless networks. Those security mechanisms include key distribution methods, cryptographic procedures, and crypto algorithms. Often the security mechanisms are so different that integration of those mechanisms is impossible.

II. RELATED WORK

A lot of work is being done in the field of routing protocols in WMNs but little effort is put up for a security management in routing protocols. However, there are some protocols which are good enough to be implemented in WMNs and provide a secure multi-path route management such as [3], [4], [5] and [6].

A secure multi-path routing protocol called Secure Routing Protocol (SRP) [3] by Papadimitratos and Haas was initially developed considering the general security of ad hoc networks. Another approach was provided by Burmester and Van Le [4], which is based on the Ford-Fulkerson maximum flow algorithm. Kotzanikolaou et al presented Secure Multi-path Routing (SecMR) [6] protocol to reduce the cost of node authentication. SecMR works in two phases: mutual authentication and route discovery phase. At the end of route discovery, the end nodes use a symmetric key in order to verify the integrity of the discovered paths. SecMR provide multiple paths along with routing security and is better than the other two protocols. However, due to the use of digital signature in periodic mutual authentication phase, the computation cost and control overhead incurred render this scheme inefficient. Michael Weeks and Gulshan Altan have provided a secure and efficient version of Dynamic Source Routing (DSR) in [5]. However, their security mechanism uses a shared network key, which is a single point of failure (if compromised), in the network. There scheme also provide secured communication using public key cryptography, which again results in high computational cost and delay. In paper [7], a security management mechanism for multi-path routing is utilized which efficiently uses the characteristics of WMNs, mutual authentication and secrete key cryptography to provide secure multi-path route management. This scheme takes less overhead than the available secure multi-path routing mechanisms but as they are using Diffie-Hellman[11], there is a danger that a third party might intercept the packets in between. So we propose an algorithm which is stronger than [7].

III. BASIC SECURITY ISSUES

To ensure the security of WMNs, the following major security objectives of any application have paramount importance.

- Confidentiality - It means that certain information is only accessible to those who have been authorized to access it. In other words, it ensures that certain information is never disclosed to unauthorized entities
- Integrity - Integrity guarantees that a message being transferred is never corrupted. Integrity can be compromised mainly in the following two ways:

  Malicious altering – A message could be removed, replayed or revised by an adversary by a malicious attacker

  Accidental altering - such as a transmission error goals on the network, which is regarded as malicious altering.
- Authenticity - Authenticity is essentially assurance that participants in communication are genuine and not impersonators.
- Non-repudiation - Non-repudiation ensures that the sender and the receiver of a message cannot deny that they have ever sent or received such a message. It is useful for detection and isolation of a node with some abnormal behavior.
- Authorization - Authorization is a process in which an entity is issued a credential by the trusted certificate authority. It is generally used to assign different access rights to different level of users.
- Anonymity - Anonymity means that all the information that can be used to identify the owner

or the current user entity should be kept private and not distributed to other communicating parties. This security requirement is closely related to the preservation of privacy.

IV. PROPOSED SECURITY FRAMEWORK

Before turning to our technical content, we first put our work in context. The vast literature on WMN security contains valuable proposals. We narrow our focus to environments with the following characteristics: a very large number of nodes with a relatively high density, a very general communication pattern.

The core of this paper describes an algorithm for building a secure Hybrid WMN employing cryptographic extension to provide authenticity and integrity of messages. For this, we should first identify the ***security reference points***, which are broadly categorized as :

- *Inter-network* – These are the boundaries between the heterogeneous networks i.e. a client in one type of network is communicating with the client in other type of network.
- *Intra-network* – This is a security point between devices with a single network domain. Before a client could access a network, he must first be authenticated by the serving network.

A. ASSUMPTIONS

- We assume that WMN has a hierarchical structure with mesh router making routing infrastructure and mobile wireless clients making up ad hoc networks at the second level of the network.
- Each ad hoc network of wireless mesh clients has one or more routers from the router infrastructure in ad hoc region. These router nodes are powerful enough to provide management functionality to the wireless mesh network.
- The routers which are connected with the clients are called manager routers and the nodes in client mesh are called client nodes. Each manager router has a parent mesh router which in turn has a parent. This continues till the parent of a router is a IGW (Internet Gateway).
- Each manager router is responsible to provide routing assistance, mobility management and security management to its mesh client network.
- There is a Certification Authority (CA) in the WMN which is a trusted third party that can authenticate the digital certificates of the nodes.
- We also assume that a Social Security Number(SSN) which is used to identify the clients personal details containing his identity information (like name, father's name, address, passport number, blood group, phone number, gender, date of birth, etc.) is maintained globally in all the countries where internet is accessed. It is an entry ticket to access the Internet. Any SSN can be used only by a single user i.e. simultaneously two persons cannot use the same SSN number. This SSN along with a password is maintained at state level in which a person resides. We propose that such a data should be kept in the form of distributed database that should be horizontally fragmented on the basis of states and its replicas should be maintained in its two adjacent states, i.e. one towards its left and one towards its right.

B. PROPOSED MODEL

In the proposed scheme, each mesh client network is centrally managed by a manager router with gateway. Each mesh router is assigned a digital certificate by a CA which is used to authenticate the validity of a router. Whenever a new clients enters a network, he receives a digital certificate from its manager router to prove its validity. These certificate could be verified by contacting the CA. Thereafter, the client is asked to enter its SSN (Social Security Number) along with the password through SSL encrypted web page. After verification the captive portal (government authorized web server which keeps a record of SSN details) authorizes the client to network access and assigns him a UIDN (Unique Identification Number). The UIDN generated is used to keep a record of the client's SSN, IP address and its manager router (through which it received such information). UIDN may be used to trace the person, in case some attack is detected in the network. The manager router stores the UIDN of the client along with a public key that will be sent to that client to ensure authenticity and integrity of the following messages. The router to router communication is also possible only after exchanging their corresponding digital certificates for the first time.

In the second step, both client node and its manager router encrypt the messages by their private keys before sending them to each other. This process authenticates both the nodes. Both of them can verify the authenticity of each other by contacting the CA. The secret public key which was sent at the time of assigning the UIDN is used to generate a key through Elliptic curve Diffie-Hellman algorithm that can be used for further communication. ECDH provides desired security level with significantly smaller keys. Now, for future communication the secret keys need not be entered every time. This pair of secret keys is used to provide secure multi-path routing in WMN.

C. APPLICATION SCENARIO

Let there be a WMN as shown in Fig 2. All the circles represent the nodes and edges represents the links. The cloud represents the mesh infrastructure connected to several mesh clients. The mesh client network consists of nodes A, B, C, D and R. R is a manager router and all others are client nodes. There is a CA connected to mesh infrastructure somewhere in the network.

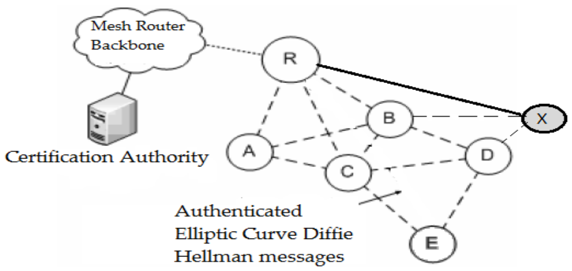

Figure 2: Mutual Authentication at the entrance of node E in mesh client network

Here is the proposed solution to the two major security reference points:

- *In the Intra- network*

Suppose a new node X comes into the mesh client. First, the manager router sends a digital certificate to prove its authenticity. Upon receiving it, X sends its SSN and password (via SSL) to R, which is sent to the authorized portal for verification. If the information is valid, a UIDN is generated and stored by the portal along with its corresponding SSN, IP Address and router information. This UIDN is then sent to R. R stores the UIDN of that client and sends a secret key to X, this is the first step in the generation of keys using Elliptic Curve Diffie-Hellman. To engage in secure communications with ECDH, both X and R chooses –

- The parameters q, a, and b for an Elliptic Curve based Group Eq(a, b) where q is a prime or an integer of the form 2^m.

- A base point P є Eq(a, b) whose order is a large value n. The value of n is also a part of the information that must be made publicly available

X	R .
• Choose private key **b** < n	Choose private key **a** < n
• Compute $\mathbf{Q_X} = \mathbf{bP}$	Compute $\mathbf{Q_R} = \mathbf{aP}$
• Send $\mathbf{Q_X}$ to R	Send $\mathbf{Q_R}$ to X
• Compute $\mathbf{K}= \mathbf{bQ_R}$	Compute $\mathbf{K} =\mathbf{aQ_X}$

We can see that $\mathbf{K} = \mathbf{bQ_R} = \mathbf{abP} = \mathbf{aQ_X}$. Now R and X have the shared secret key **K** that could subsequently be used for, say, a symmetric-key based communication link. To discover the secret key, an attacker could try to discover the key K from the publicly available base point P and the publicly available Q_X or Q_R. But this requires solving the discrete logarithm problem which, for a properly chosen set of curve parameters and P, can be extremely hard. To increase the level of difficulty in solving the discrete logarithm problem, we can select for P, the order which is very large. The order of a point on the elliptic curve is the least number of times G must be added to itself so that we get the identity element 0 of the group Eq(a, b).

- *In the Inter-network*

Most of the traffic in WMN flows through the Gateway for internet access, so the scenario presented would suffice that type of access. But if a client node in one type of network wants to transmit information to a client in another type of network, then a second phase is needed. In the second phase of the security framework, the source manager router and the destination manager router run 2-party ECDH(Elliptic Curve Diffie-Hellman) in parallel with source and destination. Suppose a client A with manager router R1 wants to transmit information to B with manager router R2. If A and R1 possesses a shared secret key abP for transmission and B and R2 possesses a shared secret key cdP. Then, for exchanging the information between A and B, first the message is encrypted using the key, abP from A to R1. Then for transmission from R1 to R2, again ECDH algorithm is executed, where R1's private key is generated as ab * x and R2's private key is generated as cd * y (x and y are randomly generated integers that are used to enhance the security against eavesdropping). So the shared secret key between R1 and R2 is abxcdyP which can be used for secured transmission in an inter-network. R2 decrypt it, and again encrypt it using the key cdP and send it to B. After this process, four nodes can communicate securely.

D. MOBILITY AND ADDRESS MANAGEMENT

As the WMN clients are mobile, they may change position from one ad hoc region to the other. Whenever, a node changes its network from one manager router to the other, the whole process is started again i.e. first the router will produce its certificate, then the key generation algorithm is started again. This is needed to ensure security as the entire key might be eavesdropped in between. The UIDN is not generated again for the same session, it is passed from the previous router to the new one and the change of location is intimated to the IGW for updating.

E. SECURITY ANALYSIS

Security is one of the critical concerns of every network. Resource consuming public key cryptography is not feasible for the client nodes. Our proposed mechanism presents an efficient way of reducing the security overheads. ECC used in our model provides the same security as a 1024 bit RSA algorithm, and can be anywhere from 5 to 15 times faster depending on the platform and consumes very less energy [8]. And once, the router is authenticated and keys are exchanged, all further messages are encrypted with the same keys. If somehow, some attacker succeeds in breaching the security and is detected, he could be traced by its SSN entered at the time of registration and with the help of the UIDN his location can be traced. Thereafter, the SSN is recorded and debarred for any further access to internet through any device.

Our mechanism is secure enough that if a node is compromised then the whole network does not get affected by it. As all nodes communicates with each other with separate secret keys so, if a node is compromised and tries to adverse the network it is not possible for the node to be much hostile to the rest of the network. If there is a compromised node in the network, then there are two possibilities of an adversary node being in the network. In case 1, a node outside the network tries to attack the routing mechanism. Case 2 is the scenario in which the node entering the network is already a compromised node or the node is compromised during its participation in the network (such as due to the lack of physical protection etc). In the first case, the messages by the compromised node would not be accepted by the other nodes as it cannot be authenticated by them. So the adverse messages would be dropped by the nodes as they cannot verify the adverse node as a member node. The second case can be harmful for the network as other nodes can verify the compromised node as a decent node. This node can communicate with its neighbor nodes and can inject false information in the network. But this compromised node cannot listen to other nodes' communications and cannot affect them. So if a node is compromised in the network all the other nodes are safe from this node and can communicate with other nodes securely. As our mechanism is for a multi-path routing protocol, hence, the messages are secure from the adversary as there are several paths to evade the compromised nodes. Even if the adversary have '*n*' compromised nodes with every compromised node is in a different path then with '*m*' paths in between two nodes, adversary require $n \varepsilon m$.

F. ROUTING ASSISTANCE

UIDN for mobile clients are allocated dynamically by the IGW of that region. This number defines the location of that mobile client i.e. in which ad hoc region the mobile node is present. Our mechanism will help in routing, as the border router manages the addresses and monitors the network, it can help in routing decisions. The manager router can find the optimum paths between two nodes, detect link losses and find alternate paths within the client mesh network. Geographic routing is possible with the help of UIDN as it helps in making the decisions as to which node it should forward the data to reach the destination.

V. SIMULATION AND ANALYSIS

We compared our security mechanism with the SRP [3], secure multi-path routing protocol of Burmester and Van Le [4] and SecMR [6] routing protocols. We perform the simulation of each of these security schemes. The proposed scheme is implemented with ad hoc on demand multi-path distance vector (AOMDV) [9] which is a multi-path derivative of AODV. We have compared the routing overhead of these schemes and also the amount of energy consumed by these scheme at each node. We performed the simulation in NS-2 [10]. The network model was consisted of 49 client nodes placed randomly within an area of 1000 x 1000 m_2. There are 16 mobile router nodes deployed in a grid environment to make up the mesh infrastructure. This scenario constructed 10 different mobile client networks. Each node has a propagation range of 150 meters with channel capacity 2 Mbps. The speed of mobile nodes is set to be 0 or 20 m/s. The size of the data payload is 512. Each run of simulation is executed of 900 seconds of simulation time. The medium access control protocol used is IEEE 802.11 DCF. The traffic used is constant bit rate (CBR).

From the figures given below, we observe that SRP works better than other schemes as it has less overhead and also consumes very little amount of energy. However, SRP does not provide optimal security; the intermediate nodes are not authenticated and the messages integrity is ensured by secret key cryptography. All this factors sum up to make SRP not feasible for wireless mesh networks. Scheme [4] shows high routing overhead as it contains the neighbourhood information and digital signatures with the route request. This information is increased at every node so the message size increases drastically and produces a huge amount of overhead. This scheme is good for security as well as mutual authentication but its overhead is very high; lot of energy is required at the client nodes and delay in finding the route is also high.

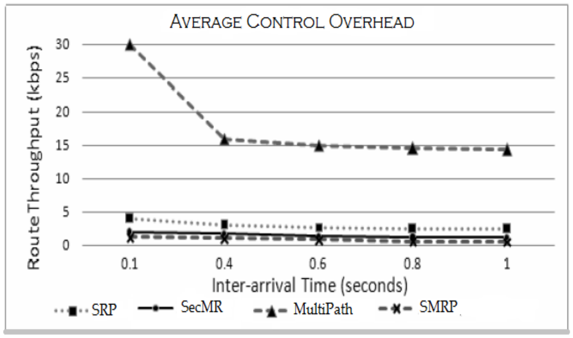

Figure 3: Comparison of Routing Overhead of various protocols

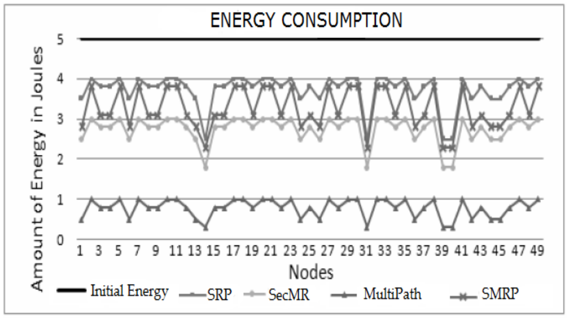

Figure 4: Amount of Energy Left after 900s simulation

In SecMR, each node mutually authenticates its neighbor node at a periodic interval and public key cryptography is used to ensure security of the messages. Although the routing phase is separated from this authentication phase but this authentication is required after a constant interval, hence a considerable amount of energy is wasted in
these periodic mutual authentications.

Our security mechanism does not require this periodic authentication, instead it uses public key cryptography only once and secret keys are used for further communication. This secret key deployment is not periodic and done after the mutual authentication by using public key cryptography. This reduces the energy consumption at each node and the routing overhead is also less than the other schemes.

VI. CONCLUSION

In summary, we have presented a security framework for hybrid WMN. Major security requirements for the hybrid mesh network are analyzed and a security framework for the integration of heterogeneous wireless networks is proposed that is secured as well as light weight which means it is suitable for energy constrained mesh client networks like sensor networks. Through simulation we have proved that our scheme is better than the existing ones.

References:

[1] From Wikipedia en.wikipe,” en.wikipedia.org/wiki/**Wireless_mesh_network**

[2]] Willie W. Lu, “Open Wireless Architecture and Its Enhanced Performance,” *IEEE Communications Magazine*, vol. 41, no. 6, pp. 106-07, June 2003

[3]. Papadimitratos, P., Haas, Z.: Secure routing for mobile ad hoc networks. In: Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS), TX, San Antonio (January 2002).

[4]. Burmester, M., van Le, T.: Secure multipath communication in mobile ad hoc networks. In: ITCC 2004, IEEE, Las Vegas (2004)

[5]. Weeks, M., Altun, G.: Efficient, Secure, Dynamic Source Routing for Ad-hoc Networks. Journal of Network and Systems Management 14(4), 559–581 (2006)

[6]. Kotzanikolaou, P., Mavropodi, R., Douligeris, C.: Secure multipath routing for mobile ad hoc networks. In: Proceedings of the WONSS05 Conference, St. Moritz, Switzerland, January 19-21 2005, pp. 89–96. IEEE, Los Alamitos (2005)

[7] M Siddiqui,”On a Low Security Overhead Mechanism for Secure Multipath Routing in Wireless Mesh Network”, APNOMS 2007, LNCS 4773, pp. 466–475

[8] Elliptic Curve Cryptography Lecture Notes on “Computer and Network Security”by Avi Kak (kak@purdue.edu)

[9] Marina, M.K., Das, S.R.: On-demand multipath distance vector routing in ad hoc networks. In: the proceedings of Ninth International Conference on Network Protocols,November 11-14, 2001, pp. 14–23 (2001)

[10] UCB/LBNL/VINT Network Simulator - ns 2, http://www.isi.edu/nsnamjns

[11] 13. Diffie, W., van Oorschot, P., Wiener, M.: Authentication and authenticated key exchange. Designs, Codes and Cryptography 2(2), 107–125 (1992)

[12]“An Integrated Security Framework For Open Wireless Networking Architecture” Jongmin Jeong And Zygmunt J. Haas, Cornell University, IEEE Wireless Communications , April 2007