Optimal Routing Service for Wireless Network security and Management

V.Senthil vel
Assistant professor/CSE
Arulmigu Meenakshi Amman College of Engineering, Kanchipuram.

S.K.Srivatsa
Sr.Professor/ECE
St.Joseph College of Engineering,Chennai.

Abstract— Wireless Network Environment Moreover, it is feasible to deploy wireless poses its unique challenges to the existing sensor networks that are able to sense and Transaction models which are fail to solve, report several physical phenomena in a real Wireless ad hoc networks (WANETs) time manner. A wireless sensor network experience serious security issues even when consists of a sensor nodes group that is solutions employ preventive or reactive miniaturized computers’ systems, security mechanisms. In order to support both interconnected by a wireless technology in an network operations and security requirements ad hoc fashion. In fact, these networks are of critical applications, we present SANA, a practical in various applications such as Secure Ad hoc Network Architecture. Its goal environmental supervision, medical care and lies in managing adaptively preventive, reactive and tolerant security mechanisms to provide essential services even under attacks, intrusions as for as communication protocols are or failures. We use SANA to design a path selection scheme for WANET routing. The evaluation of this path selection scheme considers scenarios using urban mesh network mobility with urban propagation models, and also random way point mobility with two-ray ground propagation models. Results show the survivability achieved on routing service under different conditions and attacks.

Keywords— Mesh Network, Security management, wireless ad hoc networks, survivability, routing.

I. INTRODUCTION

Now a days, with the enormous technological innovations, the low-cost sensor devices development has become possible.
network services. Secure routing and computational intensiveness. Considering cryptographic key distribution. Most of existing security solutions for WANETs [7] employ evaluation results show the mitigation on the preventive or reactive security mechanisms, detecting intrusions and thwarting attacks by cryptography, authentication and access control mechanisms [8]. Due to these limitations, researchers have developed intrusion tolerant solutions [9] as a third defense line, to mitigate the impact of attacks and intrusions by fault-tolerance techniques, typically redundancy and recovery mechanisms. However, security solutions remain still focused on one specific issue or layer of the protocol stack, being ineffective to ensure essential services of wireless ad hoc networks. Security Initially, the architectures for network management lies in one of the key research surviavility were proposed to improve both challenges on WANETs due to their security and dependability of information characteristics, critical application requirements systems in the Internet context [14]–[16], and restrictions on defense lines [10]. Security Albeit the importance of all architectures to management consists of mechanisms to control support the survivability concept, we highlight security mechanisms and services, thwarting SABER [15] and SITAR [16] architectures due attacks or intrusions. Since critical applications to their completeness in terms of survivability demand new capabilities from WANETs to properties as resistance, recognition, recovery support essential services even under attacks and adaptation. SITAR is architecture for and intrusions [11]–[13], the design of new surviving distributed services and comprises approaches for security management is a different components, such as proxy servers, demanding task. In this work, we introduce monitors, audit control module and adaptive SANA, a Survivable Ad hoc and Mesh Network Architecture, whose goal is the design of survivable essential network services against attacks and intrusions. SANA manages preventive, reactive and tolerant security mechanisms in an adaptive and coordinated way, focusing on the survivability of link-layer connectivity, routing and end-to end communication. We employ SANA for supporting the development of a survival path selection scheme on routing service.

The designed scheme is stand-alone of any protocol and consists in choosing the most any protocol and consists in choosing the most survival paths. Hence, the scheme takes into account different criteria that correlate both decentralized fashion. In the last years, network conditions and three defense lines. The association of all criteria and inferences is based on fuzzy logic due to its low survivalibility concepts have also been applied in wireless and mobile networks. Existing works can be categorized in two classes, those to
improve network survivability managing encrypted web page. After verification the mechanisms for tolerating faults and those that captive portal (government authorized web propose security management architectures to server which keeps a record of SSN details) survive intrusions and attacks [17]–[20]. In authorizes the client to network access and [17], security management architecture towards assigns him a UIDN (Unique Identification a survivable access control in WANETs is Number). The UIDN generated is used to keep proposed, being the survivability achieved by a record of the client’s SSN, IP address and its the creation of secure groups. In [18], an manager router (through which it received such architecture is defined to improve WLAN information). UIDN may be used to trace the survivability against attacks that harm access person, in case some attack is detected in the points. In [19] and [20], security management architectures for survivable wireless sensor of the client along with a public key that will be networks have been designed, focusing on DoS sent to that client to ensure authenticity and attacks and on multiple attacks, respectively. integrity of the following messages. The router However, all those architectures handle only to router communication is also possible only one specific service and do not employ more than two defense lines together, being still certificates for the first time. In the second step, unable to attain simultaneously all survivable both client node and its manager router encrypt properties, as resistance, recognition, recovery the messages by their private keys before and adaptation. correlate security criteria with sending them to each other. This process other related to network characteristics. Nie et. al [33] proposed the fuzzy logic based security-level (FLSL) routing protocol. It selects the highest security-level routes, calculated by fuzzy logic through the correlation among path length and two security characteristics, cryptographic key length and frequency of key exchanges. However, the initial FSL proposal defines a single path protocol and it does not address survivability issues.

III. PROPOSED MODEL

In the proposed scheme, each mesh client network is centrally managed by a manager router with gateway.

IV. APPLICATION SCENARIO

Let there be a WMN as shown in Fig 2. All the circles represent the nodes and edges represent the links. The cloud represents the certificate by a CA which is used to authenticate the validity of a router. Whenever a new clients enters a network, he receives a nodes A, B, C, D and R. R is a manager router digital certificate from its manager router to and all others are client nodes. There is a CA prove its validity. This certificate could be connected to mesh infrastructure somewhere in verified by contacting the CA. Thereafter, the the network. Figure 2: Mutual Authentication client is asked to enter its SSN (Social Security at the entrance of node E in mesh client Number) along with the password through SSL.

579
network Here is the proposed solution to the two major securities 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 2m.
  - A base point P ∈ 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 QX = bP Compute QR = aP
  - Send QX to R Send QR to X
  - Compute K= bQR Compute K =aQX
  We can see that K = bQR = abP = aQX. 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 QX or QR. 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 which can be used for secured transmission in an inter-network. R2 decrypt it, and again encrypt it using the key and send it to B. After this process, four nodes can communicate securely.

V. **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 it’s 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.

VI. 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 has ‘n’ compromised nodes with every compromised node in a different path then with ‘m’ paths in between two nodes, adversary require \( n \div m \).

F. ROUTING ASSISTANCE UIDN for mobile clients is 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 the message size increases drastically and of energy consumed by these scheme at each produces a huge amount of overhead. This node. We performed the simulation in NS-2 scheme is good for security as well as mutual [10]. The network model was consisted of 49 authentication but its overhead is very high; lot client nodes placed randomly within an area of of energy is required at the client nodes and 1000 x 1000 m². There are 16 mobile router delay in finding the route is also high. nodes deployed in a grid environment to make up the mesh infrastructure. This scenario In SecMR, each node mutually constructed 10 different mobile client authenticates its neighbor node at a periodic networks. Each node has a propagation range interval and public key cryptography is used to of 150 meters with channel capacity 2 Mbps. ensure security of the messages. Although the The speed of mobile nodes is set to be 0 or 20 routing phase is separated from this m/s. The size of the data payload is 512. Each authentication phase but this authentication is run of simulation is executed of 900 seconds of required after a constant interval, hence a simulation time. The medium access control considerable amount of energy is wasted in protocol used is IEEE 802.11 DCF. The traffic these periodic mutual authentications. Our used is constant bit rate (CBR). From the security mechanism does not require this figures given below, we observe that SRP 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 However, SRP does not provide optimal the mutual authentication by using public key security; the intermediate nodes are not cryptography. This reduces the energy authenticated and the messages integrity is consumption at each node and the routing ensured by secret key cryptography. All this overhead is also less than the other schemes. factors sum up to make SRP not feasible for wireless mesh networks. Scheme shows high routing overhead as it contains the neighborhood information and digital signatures with the route request.

![Energy Consumption Graph](image)

*Figure 1: Comparison of Routing Overhead of various protocols*
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 lightweight 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

Figure 2: Amount of Energy Left after 900s simulation
[29] H. Liu, J. Li, Y.-Q. Zhang, and Y. Pan, -An adaptive genetic fuzzy


