ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

Volume 3, Special Issue 3, March 2014

2014 International Conference on Innovations in Engineering and Technology (ICIET'14)

On 21st & 22nd March Organized by

K.L.N. College of Engineering, Madurai, Tamil Nadu, India

A Self Adaptive Mesh Topology with Enhanced Security for Mobile Ad-Hoc Networks Using Crypto Algorithm

Mr. B.Jaiganesh[1], S.Hamsavaahini[2], K.Janani[3], D.S.Meenaatchi[4]

K.L.N. College of Information Technology, India.

ABSTRACT- The vision of nomadic computing with its ubiquitous access has stimulated much interest in the mobile ad hoc networking (MANET) technology. These infrastructure less, self-organized networks, which either operate autonomously or as an extension to the wired networking infrastructure, are expected to support new MANET-based applications. However, the proliferation of this networking paradigm strongly depends on the availability of security provisions, among other factors. The absence of infrastructure, the nature of the envisioned applications, and the resource-constrained environment pose some new challenges in securing the protocols in ad hoc networking environments. The security requirements can differ significantly from those for infrastructure-based networks and the provision of security enhancements may take completely different directions as well. In this paper, we study the schemes proposed to secure mobile ad hoc networks.

KEYWORDS- Encrypting data, Self organized networks

I.INTRODUCTION

Wireless communication is without a doubt a very desirable service as emphasized by the tremendous growth in both cellular and wireless local area networks (WLANs) (primarily, the ones that are compliant with the IEEE 802.11 family of standards, popularly known as Wi-Fi). However, these two radically different technologies address only a narrow range of connectivity needs, and there are numerous other applications that can benefit from wireless connectivity. The cellular networks offer wide area coverage, but the service is relatively expensive and offers low data rates: even the third generation of cellular networks (3G) offers (at best) low data rates (≈2Mbps) compared to WLANs (>50Mbps for IEEE 802.11a and 802.11g and 100Mbps for proprietary solutions at the time of this writing). On the other hand, the WLANs have rather limited coverage (and the associated reduced mobility).

Furthermore, in order to increase the coverage of WLANs, a wired backbone connecting multiple access points is required. Wireless metropolitan area networks (WMANs) (e.g., the family of IEEE 802.16 standards), partially bridges this gap, offering high data rates with guaranteed quality of service to a potentially large customer base (up to tens of miles from the base station). The main drawback of WMANs is their (current) lack of mobility support and the line of sight (LOS) requirement: if a customer does not have a clear LOS to the WMAN base station, it is unlikely that he can receive service. In communities with a high density of obstructions (high-rise buildings or trees), more than half of the customers cannot be served due to the LOS requirement. Furthermore, the base stations tend to be complex and expensive. Wireless mesh networks (WMNs) have the potential to eliminate many of these disadvantages by offering low-cost, wireless broadband Internet access both for fixed and mobile users.

In its most general form (see Fig. 1), a wireless mesh network (WMN) interconnects stationary and/or mobile clients and optionally provides access to the Internet. The defining characteristic of a WMN is that the nodes at the core of the network are forwarding the data to and from the clients in a multihop fashion, thus

forming a (mobile) ad hoc network (MANET). Beyond the multihop requirement, there are no other restrictions on the design of a WMN, resulting in

currently existing solutions for such scenarios

Fig. 1 Wireless mesh network

considerable flexibility and versatility. This versatility allowed many players to enter the mesh networking arena with different products and applications. For example, the Inter-net access link in above Fig can be wired (e.g., T1, Ethernet, etc.), wireless (point to point or point to multipoint), or be absent. Some WMN technologies are designed for high-speed mobility (100mph), some for casual roaming in a building, while others are only meant to be used by stationary clients. Due to their versatility, WMNs can efficiently satisfy the needs of multiple applications such as broadband internet access and indoor WLAN coverage.

II. OVERVIEW

Nowadays, networks - communication in general - are becoming more and more important. Sadly, due to the global warming, more and more often, severe first response scenarios such as earthquakes, avalanches, and flooding happen. To rapidly organize and coordinate the res-cue forces, a working communication infrastructure is essential. Unfortunately, often the entire communication infrastructure is destroyed during the disaster or was never present in some ur-ban regions. Therefore, it would be very helpful and most-likely lifesaving, if a broadband and reliable communication infrastructure could be deployed quickly and maintained. This temporary infrastructure should be adaptable to different scenarios and should be deployable as fast and easy as possible. The

are often ground-based, which makes it very difficult to establish a working communication infrastructure in a destroyed and inaccessible area.

Our Existing solution avoids all these disadvantages: An autonomously deployable and highly adaptable flying WMN could support the rescuers and help them saving lives. The main goals of this study are the following:

Create a detailed concept how a flying WMN should be designed, developed, deployed and maintained to provide an adaptable, mobile, scalable and robust communication infrastructure. It should be deployable in a fast and easy way, even in inaccessible areas.

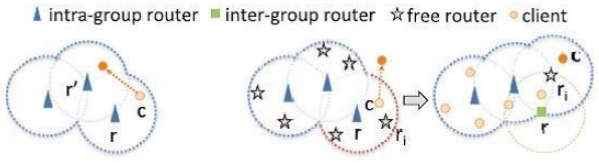
Implement and evaluate different possible network scenarios and topologies. UAVNet should cover a wide range of different applications such as a simple connection between two client devices or the coverage of large areas by multiple UAVs. Analyse the feasibility of an implementation of a working prototype within the limits of this thesis. Implement a working prototype to show the feasibility of a flying communication network. Keep the prototype as generic and expandable as possible to simplify the development and implementation of future extensions and application scenarios. Use common standard software and hardware to keep the system as cheap, compatible and lightweight as possible.

Use a user-friendly Graphical User Interface (GUI) on a mobile user device to simplify the deployment and monitoring of the network.

Evaluate the built prototype and the developed concepts and compare them to land-based approaches.

A. Existing System

Similar to stationary wireless mesh networks, an AMM-NET[1] is a mesh-based infrastructure that forwards data for mobile clients as shown in Fig. A client can connect to any nearby mesh node, which helps relay data to the destination mesh node via multi-hop for-warding. Like stationary wireless mesh networks, where routers are deployed in fixed locations, routers in an AMMNET can forward data for mobile clients along the routing paths built by any existing ad-hoc routing protocols, e.g., AODV.



(a) client moves into the radio range of another router

(b) free router r_i tracks the miss-ing client that has moved out of the current coverage

Fig.2 Client tracking in AMMNET

Unlike stationary wireless mesh networks, where routers are deployed at fixed locations, routers in an AMMNET are mobile platforms with autonomous movement capability [5]. They are equipped with positioning devices such as GPS, to provide navigational aid while tracking mobile clients. Clients are not required to know their locations, and only need to periodically probe beacon messages. Once mesh nodes receive the beacon messages, they can detect the clients within its transmission range. With this capability, mesh nodes can continuously monitor the mobility pattern of the clients, and move with them to provide them seamless connectivity as shown in Fig.2. A few assumptions are made in the design. We consider a two-dimensional airborne terrain where there is no obstacle in the target field. Mesh nodes can ex-change information, such as their locations and the list of detected clients, with their neighboring mesh nodes. The radio range of each node is not a perfect circle in an application domain with obstacles. This factor may affect the accuracy of the sensing mechanism and, to a minor degree, the coverage. However, this does not affect the general applicability of the proposed techniques for AMMNETs. For simplicity, we assume that the radio range of both mesh nodes and clients is a perfect sphere.

B. Proposed System

The characteristics of self-organization, wireless medium, and the absence of fixed infrastructure make Wireless Sensor Network (WMN) easy to set up, and thus attractive to users. However, the open and dynamic operational environment of WMN makes it very vulnerable to attacks such as denial of service attacks, radio–jamming attacks, impersonation attacks and fabrication attacks. Another common type of attacks at WMN targets at the underlying routing protocols. Because every network node in a WMN can be a router for data transmission, malicious nodes have opportunities to modify or discard routing information or even to advertise fake routes in an attempt to attract user data to go through themselves. It is understandable that the most efficient and easiest way of attacking WMN is to attack routing protocols. To address the security issues in routing in WMN, we consider social trust derived from social networks in addition to traditional quality-of service (QoS) trust derived from communication networks to obtain a composite trust metric as a basis for evaluating trust of nodes in mobile network applications. As an application of the proposed trusted routing algorithm, a novel reactive routing protocol on the basis of the standard dynamic source routing protocol, called secure source routing protocol is proposed. Several experiments have been conducted to evaluate the efficiency of the protocol in malicious node identification and attack resistance. The experimental results show that protocol can effectively detect the malicious nodes that guarantee the packet delivery ratio and the network throughput.

III.DESCRIPTION

A.Flow Diagram

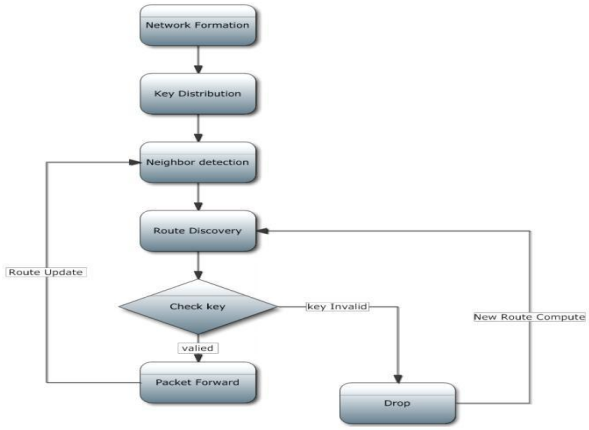


Fig.3 Flow diagram

The flow diagram given in Fig.3 shows the procedure followed in our proposed approach. First the network is formed, then the key is distributed. The route is discovered using trusted nodes and then the key is checked for validity and the transaction is done.

B. Modules

- Network Formation
- Route Discovery
- Crypto Algorithm
- Route Maintenance
- Performance Evaluation

1) Network Formation

We used ns2 simulator on Linux machine. Because, we focus on the link stability and route lifetime, no route overhead was considered in our simulation. In 870 X 870 m2area, mobile nodes exist. We used square area to increase average hop length of a route with relatively small nodes. Every mobile node is moving based on mobility data files that were generated by mobility generator module. The transmission range is fixed at 250 units. 20 nodes of them have destinations and try finding routes to their destination nodes. Maximum

speed of node is set to 10 m/sec. All nodes do not stop moving, and the simulation time is 500 sec. The number of nodes is varying from 50 to 100.

2) Route Discovery

To perform route discovery, the source node broadcasts a route request packet with a recorded source route listing only itself. Each node that hears the route request forwards the request (if appropriate), adding its own address to the recorded source route in the packet. The route request packet propagates hop-by-hop outward from the source node until either the destination node is found or until another node is found that can supply a route to the target. If the status of a link or node changes, the periodic updates will eventually reflect the change to all other nodes, presumably resulting in the computation of new routes. However, using route discovery, there are no periodic messages of any kind from any of the mobile nodes. Instead, while a route is in use, the route maintenance procedure monitors the operation of the route and informs the sender of any routing errors. Route maintenance can also be performed using end-to-end acknowledgments rather than the hop-by-hop acknowledgments described above.

3) Crypto Algorithm

Elliptic curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. The key management process used for cryptography application during data transfer.The cryptography technique used to product the node and data from different kind of attacks. Here we use the node forwarding mechanism for key management.The acknowledgment service provide the ensure the data transfer. Public-key cryptography is based on the intractability of certain mathematical problems. Early public-key systems, such as the RSA algorithm, are secure assuming that it is difficult to factor a large integer composed of two or more large prime factors. For elliptic-curve-based protocols, it is assumed that finding the discrete logarithm of a random elliptic curve element with respect to a publicly-known base point is Infeasible. The size of the elliptic curve determines the difficulty of the problem. It is believed that the same level of security afforded by an RSA-based system with a large modulus can be achieved with a much smaller elliptic curve group. Using a small group reduces storage and transmission requirements. For current cryptographic purposes; an elliptic curve is a plane curve which consists of the points satisfying the equation

$$y2=x3+ax+b,$$

along with a distinguished point at infinity. (The coordinates here are to be chosen from a fixed finite field more complicated.) This set together with the group operation of the elliptic group theory form an Abelian group, with the point at infinity as identity element. The structure of the group is inherited from the divisor group of the underlying algebraic variety. How it works depends on the cryptographic scheme you apply it to. As an example, it can be applied it to the Diffie-Hellman key exchange, which is commonly known as the Elliptic Curve Diffie-Hellman (ECDH) key agreement protocol.

Suppose Alice wants to establish a shared key with Bob, but the only channel available for them may be eavesdropped by a third party. Initially, the domain parameters (that is, (p,a,b,G,n,h) in the prime case or (m,f(x),a,b,G,n,h) in the binary case) must be agreed upon. Also, each party must have a key pair suitable for elliptic curve cryptography, consisting of a private key d (a randomly selected integer in the interval

[1,n−1]) and a public key Q (where Q=dG). Let Alice's key pair be (dA,QA) and Bob's key pair be (dB,QB). Each party must have the other party's public key (an exchange must occur). Alice computes (xk,yk)=dAQB. Bob computes k=dBQA. The shared key is xk (the x coordinates of the point).

4) Route Maintenance

As it is an on-demand routing protocol, so it looks up the routing during transmission of a packet. At the first phase, the transmitting node search its route cache to see whether there is a valid destination exists and if so, then the node starts transmitting to the destination node and the route discovery process end here. If there is no destination address then the node broadcasts the route request packet to reach the destination. When the destination node gets this packet, it returns the learned path to the source node. The route discovery process involves sending route-request packets from a source to its neighbor nodes, which then forward the request to their neighbors, and so on. Once the route-request reaches the destination node, it responds by unicasting a route-reply packet back to the source node via the neighbor from which it first received the route-request. When the route-request reaches an intermediate node that has a sufficiently up-to-date route, it stops forwarding and sends a route-reply message back to the source. Once the route is established, some form of route maintenance process maintains it in each node’s internal data structure called a route-cache until the destination becomes inaccessible along the route.

5) Performance Evaluation

of characteristic not equal to 2 or 3, or the curve equation will be somewhat

We have analyzed the throughput of our proposed system with the existing system. The plot is shown in the Fig. 4.The throughput is found to be higher than our existing system.

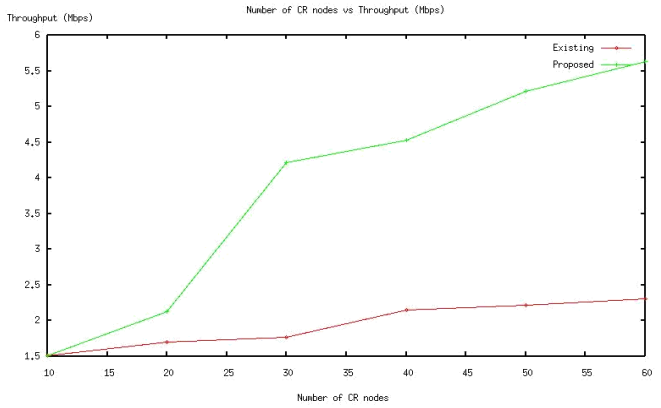


Fig.4 Throughput plot

Then packet delivery ratio of both systems were analyzed and plotted as shown in Fig.5. The proposed system shows increased packet delivery ratio.

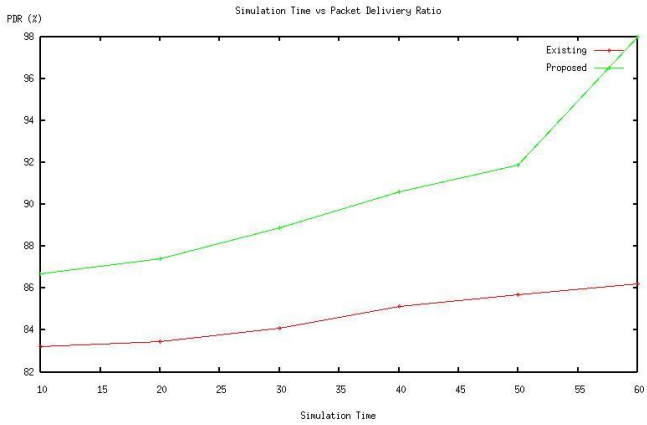


Fig.5 PDR plot

Next, we plot packet size with loss. The proposed approach shows reduced loss when compared with the existing system.

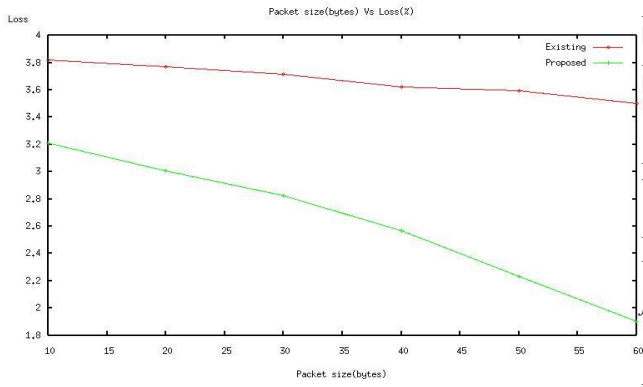


Fig. 6 Packet size vs. Loss plot

Then we plot simulation time against delay. The proposed system shows less delay than existing system.

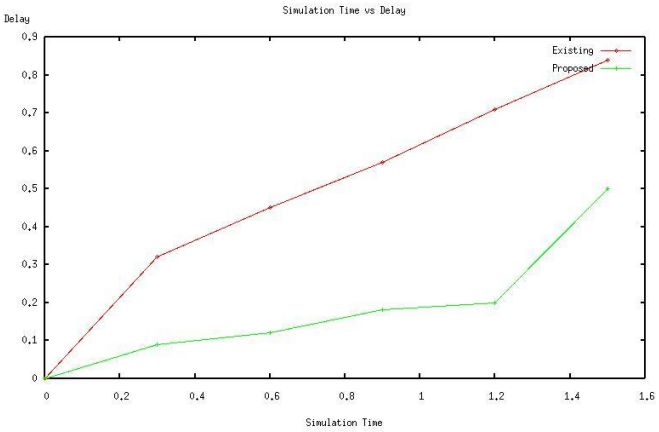


Fig.7 Delay plot

IV. CONCLUSION AND FUTURE WORK

This paper presented an analysis of Wireless Mesh Networks characteristics, security requirements, and possible communication patterns that are affected by these. By stepping back we achieved a broad overview over the security issues WMNs impose as a whole which can differ depending on the different characteristics of the network in question. We used our findings of characteristics and requirements to analyze recent security concepts for Wireless Mesh Networks. We proposed an approach which enhances security in wireless mesh networks that has increased throughput and packet delivery ratio. Future work lies in reducing the energy consumption.

V. REFERENCES

[1] Wei-Liang Shen, Chung-ShiuanChen,KateChing-Ju Lin and Kien A. Hua, *"Autonomous Mobile Mesh Networks",*
IEEE transactions on mobile computing, vol. 13, no. 2, February 2014.
[2] N. Ben Salem and J.-P.Hubaux, *"Securing Wireless Mesh Networks,"*Wireless Communications, *IEEE*, 2006
[3] S. Glass, M. Portmann, and V. Muthukkumarasamy, *"Securing Wireless Mesh Networks,"IEEE Internet Computing*, 2008.
[4]Y.-C. Hu, A. Perrig, and D.B. Johnson, "*Ariadne: A Secure On Demand Routing Protocol for Ad Hoc Networks,"Wireless Networks*, vol. 11, pp. 21-38, 2005.
[5] A. M. et al., "*Design Challenges for an Integrated Disaster Management Communication and Information System," in DIREN'*02.
[6] Y. Zhang, "ARSA: An Attack-Resilient Security Architecture for Multihop wireless Mesh Networks," Selected Areas in Communications'06
[7] M. Portmann and A. A. Pirzada, "Wireless Mesh Networks for Public Safety and Crisis Management Applications,"IEEE Internet Computing.
[8] K.E. Defrawy and G. Tsudik, "PRISM: Privacy-Friendly Routing in Suspicious MANETs (and VANETs)," Proc. IEEE Int'l Conf. Network Protocols (ICNP), 2008
[9] K.E. Defrawy and G. Tsudik, "ALARM: Anonymous Location Aided Routing in Suspicious MANETs," Proc. IEEE Int'l Conf. Network Protocols (ICNP), 2007
[10] P S Khanagoudar, "A New Autonomous System (AS) for Wireless Mesh Network",International Journal of Engineering and Innovative Technology (IJEIT)Volume 2, Issue 1, July 2012.
[11] Donggang Liu, Peng Ning, "Establishing Pairwise Keys in Distributed Sensor Networks", CCS '03 Proceedings of the 10th ACM conference on Computer and communications security,2003.
[12] L. Gong and D. J. Wheeler, "A Matrix Key-Distribution Scheme," Journal of Cryptology, 1990.

[13] A. Raniwala and T.-C.Chiueh, "Architecture and Algorithms for an IEEE 802.11-Based Multi-Channel Wireless Mesh Network,"Proc. IEEE INFOCOM, 2005.