International Journal of Engineering Inventions
ISSN: 2278-7461, ISBN: 2319-6491
Volume 1, Issue 12 (December 2012) PP:45-50

Study On Anonymous – Privacy User Communication in Wireless Mesh Networks

Mr. B. Santhosh[1], V. Anitha[2], P.Ravali[3], Mr. R V S Anil Kumar[4]

Abstract:–Connecting the networks users aware of the security and privacy is an importance to gain anonymity. The term anonymity can hide actual content of end users while allowing their access of service networks moreover they are allowed to do so without being traced. Anonymity achieve misbehaving users are the two conflicts. Our analysis provides protection in wireless mesh networks from signatures and anomalies. Implementation shows the access control of logon credentials which is secure transfer data from node to router cluster and comparative study is to achieve stronger privacy protection, anonymous to mesh routers is best effort in security performance.

Keywords:–Wireless Mesh Networks, Ad-hoc network, security, anonymous.

I. INTRODUCTION

Wireless mesh networks privacy and anonymity issues have become popularity is provided in the survey [2] that reviewed great issues on various functions. WMNs have become reliable technology that will have good future in the years to come. The security in such networks has been reviewed on various kinds of networks like cellular networks WLANs, MANETs, WSNsand VANETs. The security of anonymity in any kind ofnetworks, user's credentials has to be unlinked to his activities for each system [1], [2] and Peer-to-Peer payment systems described. The anonymous networks, itis required to hide the location information of user also to ensure that the movement of the user is not tracedas this is conceived with respect to mobile networks asreviewed in [3] and VANETs, thus routing anonymity is capable of concealing the communication between parties.It achieves it to establishing anonymous path betweenthe parties and the problem with complete anonymity withouttraceability is that insider attacks might be increased tobreak security of IT system. For this reason it is essential tohave traceability facility in case of misbehaving users [1].Wireless co-operative communication infrastructure between a massive amount of individual wireless transceivers (i.e. a wireless mesh). This type of infrastructure is decentralized, relatively inexpensive, and very reliable and resilient, as each node need only transmit as far as the next node. Nodes act as repeaters to transmit data from nearby nodes to peers that are too far away to reach, resulting in a network that can span large distances, especially over rough or difficult terrain. WMNs are extremely reliable, as each node is connected to several other nodes. If one node drops out of the network, due to hardware failure or any other reason, its neighbors simply find another route. Extra capacity can be installed by simply adding more nodes.Anonymity in sensor networks means preventing a thirdparty other than the message sender and the base stationknowing the identity of the two primary parties in a communication. Anonymizing sensor nodes can confuse adversaries about which sensor is the real sender of a message. To protect the real ID of each sensor, pseudonyms can be used for sensor nodes instead of real IDs, however, using fixed pseudonyms cannot prevent leaking identity information of sensor nodes because a long term passive eavesdropper can deduce the topology of the network through traffic analysis.

2. Related Work:

Quality security and privacy are important issues in any communication network have worked on these two areas as compared to MANETs and wireless sensor networks have received very attention. For client authentication andaccess control to guarantee a high-level of flexibility and transparency to all users in awireless network, the users can access the mesh network without requiring anychange in their devices and software. However, client mobility can pose severe problemsto the security architecture, especially when real-time traffic is transmitted. Tocope with this problem, proactive key distribution has been proposed.Providing security in the backbone network for WMNs is another important challenge.Mesh networks typically employ resource constrained mobile clients, which aredifficult to protect against removal, tampering, or replication. If the device can beremotely managed, a distant hacking into the device would work perfectly [7]. Accordingly,several research works have been done to investigate the use of cryptographictechniques to achieve secure communication in WMNs. In [8], security architecturehas proposed that is suitable for multi-hop WMNs employing PANA (Protocolfor carrying Authentication for Network Access) [9]. In the scheme, the wirelessclients are authenticated on production of the cryptographic credentials necessary tocreate an encrypted tunnel with the remote access router to which they are associated.Even though such framework protects the confidentiality of the information exchanged,it cannot prevent adversaries to perform active attacks against the networkitself. For instance, a malicious adversary can replicate, modify and forge the topologyinformation exchanged among mesh devices, in order to launch a denial of serviceattack. Moreover, PANA necessitates the existence of IP addresses in all the meshnodes, which is poses a serious constraint on deployment of this protocol.Authenticating transmitted data packets is an approach for preventing unauthorizednodes to access the resources of a WMN. A light-weight hop-by-hop access protocol(LHAP) has been proposed for authenticating mobile clients in wireless dynamic environments,preventing resource consumption attacks [10]. LHAP implements lightweighthop-by-hop authentication, where intermediate nodes authenticate all the packetsthey receive before forwarding them. LHAP employs a packet authentication techniquebased on the use of one-way hash chains. Moreover, LHAP uses TESLA [11]protocol to reduce the number of public key operations for bootstrapping and maintainingtrust between nodes.

II. SECTION

3. Problem Definition:

Connectivity for wireless mesh networks is become a problem of security and privacy to protect with signatures and hackers, existing work shows the privacy protection for ad-hoc networks it was not applicable for wireless mesh networks. Provide the antivirus, security software in the our networks the system is more complex to avoid all these issues our proposed system introduces two schema with the anonymous user credentials to connect wireless mesh network which provides security and privacy.

3.1. Network Model:

Consider the wireless mesh network under the control of a network operator it deploys a number of static mesh routers that covers the whole area to provide network services to network connectivity users. Mesh router constantly exchange topology information to every system and maintain the global information of the whole wireless mesh network. Network users for services and utilize the mobile clients to freely access the network and communicate with their peers from anywhere within the city. The membership network users may be terminated according to user operator agreement in a periodic and dynamically revoked by the user credentials.

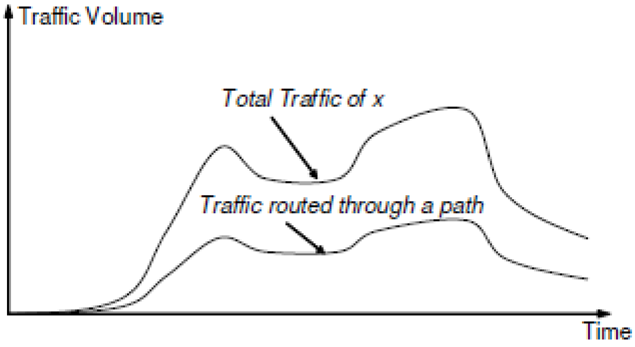


Figure 1 shows the Network Traffic

The complete traffic pattern information of x could still be obtained by a single node in case of multi-path routing. In the example shown by Figure 1 g allocates the traffic to x via three disjoint routes by fixed proportion. Any path, although only seeing one third of the flow, the observed traffic shape is isomorphic to the original one. Therefore, the traffic to x must be distributed along multiple routes in a time-variant fashion, such that the traffic pattern observed at any node is statistically deviant from the original pattern.

3.2. Anonymity:

Anonymity refers to concealing the identities of participants in all documents resulting and deciding whether or not sensitive information should be recorded. Anonymous should be respected unless a clear understanding to the contrary has been reached. Providing anonymity of information collected from research participant’s means that either the project does not collect identifying information of individual subjects or the project cannot link individual responses with participant’s identities

Thisanonymousprotocol is used to find how a message is anonymously delivered from a source node to a destination node.

The delivery of a message consists of three steps

1) Uplink Routing(Node→Router)
2) Router-Router Routing(Router→Router)
3) Downlink Delivery(Router→Node)

User Registration is Identity of a network User. It Avoids Network-Wide flooding by allow each network user to register at Mesh routers.

3.3. Key Establishment Protocol

The user broadcasts a message within his neighborhood to initiate the local key establishment protocol. Each of his neighbors replies to the initiation message and derives session keys from the messages. For privacy protection, this protocol makes use of the group-signature technique to achieve anonymous authentication.

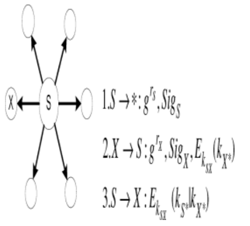

X
S
$1. S \rightarrow * : g^{r_S}, Sig_S$
$2. X \rightarrow S : g^{r_X}, Sig_X, E_{k_{SX}}(k_{X*})$
$3. S \rightarrow X : E_{k_{SX}}(k_{S*} \| k_{X*})$

Figure 2 Key Establishment

3.4. Node-to-Router Path Finding and Registration Protocol

This Protocol is used to establish the route between mesh client and mesh router, then registers the client to the mesh Router. This protocol consists of three steps. In the first step, the source node broadcasts a route request throughout the subnet to which it belongs, and the request would reach the nearest mesh router under the protection of session keys. Then, the mesh router registers the node and puts it into its user list in the second step. This information is exchanged among mesh routers so that every mesh router knows how to reach a specific node. Next, the mesh router sends a reply to the source node and the route is constructed when the reply successfully reaches the source node.Suppose a source node. *S* needs to find a route to the nearest mesh router *R*.Without loss of generality, we assume that there are three intermediate nodes *A*, *B*, and *C* between *S* and R,as illustrated in Fig.3

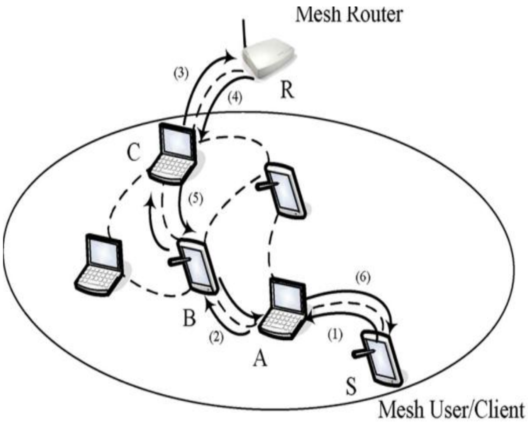


Figure 3 Node-Router Path Finding.

III. SECTION

4.1 Implementation Performance:

Wireless mesh network is characterized into low power mobile devices and low bandwidth wireless channels. Our anonymous communication protocol for wireless mesh networks on simulator ns2 and its performance comparing it with the ad-hoc On-demand distance vector mesh routing protocol.

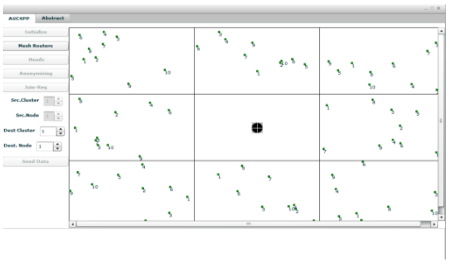
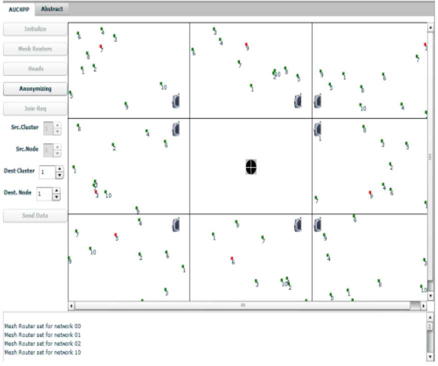
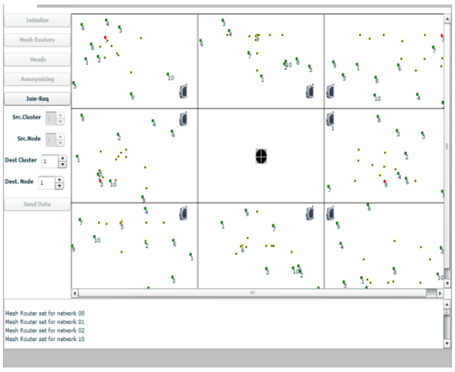


Figure 4.1 Initialize the Nodes for routing



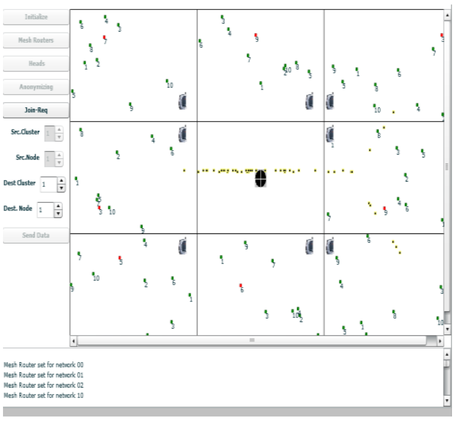
```
Mesh Router set for network 00
Mesh Router set for network 01
Mesh Router set for network 02
Mesh Router set for network 10
```

Figure 4.2 Selection of the Node-routerand clustering



```
Mesh Router set for network 00
Mesh Router set for network 01
Mesh Router set for network 02
Mesh Router set for network 10
```

Figure 4.3 Anonymous Routing



```
Mesh Router set for network 00
Mesh Router set for network 01
Mesh Router set for network 02
Mesh Router set for network 10
```

Figure 4.4 Anonymous Node routing to final Base station

Fundamental security objectives such as authentication data integrity confidentiality have been achieved easily. To achieve this digital signature message authentication code encryption code are used. Gateway or mesh router cannot establish clients real identity which is to ensure anonymity and authentication process.

The communication takes place between client and gateways while authentication, security has four intra-domain protocols that make the communication possible. The result of this proper communication is the ability of the architecture to ensure anonymity to honest user and traceability to misbehaving user. An important observation in the proposed system is that the protocols make use of symmetric keys locally. Therefore no additional communication overhead is involved. Moreover, the role of TA can be split logically into multiple servers thus the communication overhead ofthe proposed architecture is considered acceptable.TA is capable of using multiple servers for storage.Storage in these servers is not a problem of concern, during protocol execution stage, storage takes place at lowend client side. This is the concern and discussed here.There is trade-off between storage and computationaloverhead. When tickets are issued the client stores 621bytes for each protocol instance. When protocol is beingexecuted, the mesh routers do not store information.However, they store information required for inter-domainaccess. Parameters cause the large portion of overhead withrespect to storage. Analysis, thecomputational overhead that has been revealed at clientside is of interest now. Such tasks at client include hashoperations, point additions and multiplications, and alsopairing operations. Out of all these things, the pairingoperations are more computational expensive. In case ofticket issuance, the client computes two basis pairings. Thisis done in real time for each protocol instance. Theremaining computational overheads can be computed onceor can be done later. From the analysis of the computations,it can be concluded that the protocol real time intensity is acceptable.

4.2. Comparative Study:

The WMN users are the city/community residents, and they may frequently communicate with each other for various purposes. Their communications, inevitably,contain large amount of user privacy information that should be protected from malicious attackers and other network entities.Addressing this issue in WMNs is both new and challenging for a number of reasons. First, a metropolitan WMN usually has a huge network size (on the order of thousands), which limits the applicability of traditional anonymous routing protocols designed for small-size mobile ad hoc networks (on the order of hundreds). This is because traditional anonymous routing protocols for ad hoc networks usually assume pre-established trust among all network nodes to find/establish secure routing paths. However, in a metropolitan WMN, it is impossible to assume the pre-established trust relationship among all network users.

Second, existing anonymous routingprotocols for ad hoc networks do not enforce network access control, but in the WMN network, access control is essential for both security and billing purposes, as well as prohibiting network resource abuse. Last, but not least, most existing anonymous routing protocols rely on networkwide flooding for routing establishment. While expensive,network-wide flooding is not a big concern in ad hoc networks because of their small size and light traffic load. However,flooding in the WMN will waste a large amount of precious network bandwidth resources, given its huge network size and heavy traffic load. Compare to this previous work our basic scheme makes use of group signatures to anonymously establish session keys and enforce access control. In the first phase of the scheme, each mesh client anonymously constructs session keys with its neighboring nodes using group signatures. Then, these session keys are used for mesh clients to find routes to the nearest mesh router and have their identities registered. The registered identities are then used for route discovery within the mesh backbone. In this scheme, the user's identities are protected from eavesdroppers but known by mesh routers because of routing in the mesh backbone. In the advanced protocol, we make use of pairwise shared secrets along with group signatures to keep mesh clients anonymous from mesh routers hence, the advanced protocol suite achieves stronger privacy protection.

IV. CONCLUSION

Our analysis presents the privacy preserving routing in wireless mesh network and two routing schemes to provide anonymity for authentication and security. To protect from group of signatures first stage anonymously constructs session keys which are used for privacy routing discovery. Anonymous protocol mesh routers are still able to identify mobile users and track them to design and keep mobile users anonymous against mesh routers. Implementation and comparative work show that the proposed protocols are secure privacy preserving and best effort.

REFERENCE

1) European Telecomm. Standards Inst. (ETSI), ―GSM 2.09: SecurityAspects,‖ June 1993.
2) P. Kyasanur and N.H. Vaidya, ―Selfish MAC Layer MisbehaviorinWireless Networks,‖ IEEE Trans. Mobile Computing, vol. 4, no. 5,pp. 502-516, Sept. 2005.
3) D. Boneh, X. Boyen, and H. Shacham, "Short group signatures," in *ProcAdv. Cryptology–CRYPTO,* vol. 3152, *Lecture Notes in Computer Science*,2004, pp. 41–55.
4) A. Boukerche, K. El-Khatib, L. Xu, and L. Korba, "SDAR: A securedistributed anonymous routing protocol for wireless and mobile ad hocnetworks," in *Proc. 29th Annu. IEEE Int. Conf. Local Comput.Netw.*,Nov. 2004, pp. 618–624.
5) S. Capkun, J. Hubaux, and M. Jakobsson, "Secure and privacy preservingcommunication in hybrid ad hoc networks," Swiss Fed.Inst. Technol.,-DI-ICA, Lausanne, Switzerland, 2004.

6) D. Chaum and E. van Heyst, "Group signatures," in *Proc. Adv.Cryptology—EUROCRYPT*, vol. 547, *LNCS*, 1991, pp. 257–265.

7) W.Dai,Crypto++Benchmarks.[Online].Available:http://www.cryptopp.com/benchmarks.

8) D. B. Johnson and D. A. Maltz, "Dynamic source routing in ad hoc wirelessnetworks," in *Mobile Computing*, vol. 353. Norwell, MA: Kluwer,1996, pp. 153–181.

9) J. Kong and X. Hong, "ANODR: Anonymous on demand routing withuntraceable routes for mobile ad-hoc networks," in *Proc. 4th ACM Int.Symp. Mobile Ad Hoc Netw.Comput.*, 2003, pp. 291–302.

10) S. Li and A. Ephremides, "Anonymous routing: A cross-layer couplingbetween application and network layer," in *Proc. CISS*, Mar. 2006,pp. 22–24.

11) W. Lou and K. Ren, "Security, privacy, and accountability in wirelessaccess networks," *IEEE Wireless Commun. Mag.*, vol. 16, no. 4,Aug. 2009.

12) [12] Microsoft, Self-Organizing Neighborhood Wireless Mesh Networks.[Online]. Available: http://www.research.microsoft.com/mesh/

13) A. Pfitzmann and M. Hansen, Anonymity, Unobservability, andPseudonymity: A Consolidated Proposal for Terminology, Draft,Jul. 2000.

14) L. Qian, N. Song, and X. Li, "Secure anonymous routing in clusteredmultihop wireless ad hoc networks," in *Proc. CISS*, Mar. 2006,pp. 1629–1634.

15) K. Ren and W. Lou, "A sophisticated privacy-enhanced yet accountablesecurity framework for wireless mesh networks," in *Proc. 28th Int. Conf.Distrib.Comput. Syst.*, 2008, pp. 286–294.

Mr. B. SANTHOSH, Assoc. Prof., M.Tech. Computer Science &Engineering from **Hyderabad Institute of Technology and Management, Medchal** having several years of experience in various Engineering Colleges has guided many UG & PG students. Currently he is **head of the department CSE** at **Brilliant Institute of Engineering & Technology**; his areas of interest include Unix Operating System, Information security, Object Oriented Analysis & Design, Distributed Data Bases.

V. Anitha B.Tech Computer Science Engineering from BhojReddyWomen's Engineering Collegeof Engineering M.Tech Computer Science Engineering from Nishitha College of Engineeringhaving several years of experience in various Engineering Colleges has guided many UG & PG students. Currently she is AsstProfessor in ACE EngineeringCollege JNTUH and research areas include Wireless Networks & Network Security.

P.RavaliM.Tech. Computer Science & Engineering from **Hyderabad Institute of Technology and Management, MedchalB.Tech**. Computer Science & Engineering from **Hyderabad Institute of Technology and Management, Medchal**having several years of experience in various Engineering Colleges has guided many UG & PG students. Currently she is Asst Prof Teegala Krishna Reddy Engineering College, her areas of interest include Unix Operating System, Information security, Object Oriented Analysis & Design, Distributed Data Bases.

Mr. R V S ANIL KUMAR, Asst. Prof., B.Tech. Information Technology from **Dr. Paul Raj Engg.College, Bhadrachalam** and completed **M.Tech** in Computer Science and Engineering from **Kshatriya College of Engg., Armoor**. He has 5+ years of teaching experience in Engineering colleges. Currently he is at **Brilliant Institute of Engineering & Technology**. His interested areas are Databases, Object Oriented Analysis & Design, Computer Networks & Information security.