International Conference on Technologies for Sustainability- Engineering, Information Technology, Management and the Environment
DAV Institute of Management, Faridabad (SUSTECH-15)
28 November 2015 www.conferenceworld.in ISBN: 978-81-931039-7-5

ENABLING ACCOUNTABLE ANONYMOUS USER COMMUNICATION IN WIRELESS MESH NETWORK

P.Ramya

Lecturer, Dept of CS & IT, Nadar Saraswathi College of Arts & Science, Theni

ABSTRACT

Wireless mesh networks (WMNs) have recently attracted increasing attention and deployment as a promising low-cost approach to provide last-mile high-speed Internet access at metropolitan scale. Security and privacy issues are of most concern in pushing the success of WMNs for their wide deployment and for supporting service-oriented applications. Due to the intrinsically open and distributed nature of WMNs, it is essential to enforce network access control to cope with both free riders and malicious attackers. Dynamic access to WMNs should be subject to successful user authentication based on the properly preestablished trust between users and the network operator; otherwise, network access should be prohibited. On the other hand, it is also critical to provide adequate provisioning over user privacy as WMN communications usually contain a vast amount of sensitive user information. The wireless medium, open network architecture, and lack of physical protection over mesh routers render WMNs highly vulnerable to various privacy-oriented attacks. These attacks range from passive eavesdropping to active message phishing, interception, and alteration, and easily lead to the leakage of user information. As such existing routing protocol designed to provide security and privacy protection. But still, the wide deployment of WMNs can succeed only after users are assured for their ability to manage privacy risks and maintain their desired level of anonymity.

I. INTRODUCTION

Wireless mesh networks (WMNs) have recently attracted increasing attention and deployment as a promising low-cost approach to provide last-mile high-speed Internet access at metropolitan scale . A typical metropolitan WMN, consists of a group of mesh routers that form a wireless backbone and a large number of mesh clients (i.e., network users1) directly or indirectly connected to these mesh routers. The wireless backbone network formed by the mesh routers provides high-bandwidth communication channels to mesh clients connected to it. On the other hand, the mesh clients themselves form multihop wireless ad hoc networks to furthermore extend the wireless connectivity. WMNs expands coverage of wide-area cellular networks with the ease of local-area Wi-Fi networks . The advantages of WMNs also include low deployment costs, self-configuration and self maintenance, good scalability, high robustness, etc. .

Security and privacy issues are of utmost concern in pushing the success of WMNs for their wide deployment and for supporting service-oriented applications. Due to the intrinsically open and distributed nature, WMNs are subject to various attacks. Anyone with an appropriate transceiver can eavesdrop, inject, or impersonate as others in a WMN. Rogue mesh routers can easily be set up to phish user connections and traffic. All these attacks pose a great threat on user privacy protection. Ina metro scale community mesh network, the residents access the WMN from everywhere within the community, such as offices, homes, restaurants, hospitals, hotels,

shopping malls, and even vehicles. Through the WMN, they access the public Internet in different roles and contexts for services like e-mails,e-banking, e-commerce, and web surfing, and also intensively interact with their local peers for file sharing, teleconferencing, online gaming, instant chatting, etc. Obviously, all these communications contain various kinds of sensitive user information like personal identities, activities, location information, movement patterns, financial information, transaction profiles, social/business connections, and so on. Once disclosed to the attackers, this information could compromise any user's privacy and, when further correlated together, can lead to even more devastating consequences. Hence, securing user privacy is of paramount practical importance in WMNs.

II. RELATED WORK

A wireless mesh network (WMN) is a communications network made up of radio nodes organized in a mesh topology. It is also a form of wireless ad hoc network. Wireless mesh networks often consist of mesh clients, mesh routers and gateways. The wireless medium, open network architecture, and lack of physical protection over mesh routers render WMNs highly vulnerable to various privacy-oriented attacks. These attacks range from passive eavesdropping to active message phishing, interception, and alteration, and easily lead to the leakage of user information. Obviously, the wide deployment of WMNs can succeed only after users are assured for their ability to manage privacy risks and maintain their desired level of anonymity.Capkun et al. have given a privacy-preserving scheme for the so-called hybrid ad hoc networks, which are actually WMNs. The main objective of their scheme is to provide anonymity and location privacy for mobile nodes in hybrid ad hoc networks (WMNs).

In recent literature title "Achieving privacy in mesh networks" discussed a structure called "Onion ring" is proposed to achieve routing privacy in WMNs. This scheme uses "Onion encryption" in a ring structure so that it is impossible for an adversary, even a global adversary, to distinguish the source node or the destination node. This scheme is able to identity the misbehaving nodes in order to evict them.The solution discussed by Capkun in that identifiers of mobile nodes have to be disclosed to access points so that some access point may be able to track a specific mobile user. On the other hand, an adversary is able to link messages by source and destination pseudonyms, which keep unchanged within a time slot. Moreover, the attacker is assumed to have only partial knowledge but not global knowledge of the network. In the "onion ring" solution, it is not clear how to anonymously construct the ring in the first place, and furthermore, topology dynamics may make the scheme too inefficient.

III. PROPOSED WORK

In this paper, I proposed two implementation for enabling security and privacy protection in WMNs. The first scheme relies on group signatures, together with user credentials, to deliver security and privacy protection. By enforcing access control using user credentials, the user's identity has to be disclosed to mesh routers. To avoid this, our second scheme employs pair-wise secrets between any two users to achieve stronger privacy protection. In the second scheme, the user is kept anonymous to mesh routers.

• Network Access Security and Anonymity: It achieves explicit mutual authentication and key establishment between users and mesh routers and between users themselves. It thus prohibits both illegal network access from

free riders and malicious users and phishing attacks due to rogue mesh routers. It simultaneously enables unilateral anonymous authentication between users and mesh routers and bilateral anonymous authentication between any two users in a single protocol suite. It thus ensures user anonymity and privacy.

• User Accountability: It enables user accountability, aimed at regulating user behaviors and protecting WMNs from being abused and attacked. It can always audit network communications in the cases of disputes and frauds. It further allows dynamic user revocation so that malicious users can be evicted.

• Sophisticated User Privacy: It allows users to disclose minimum information possible while maintaining accountability. It allows privacy-aware secure user communication, while satisfying the above two capabilities simultaneously.

In the context of privacy-aware secure user communication research focused on the long-term security framework for WMNs. Particularly, successful to establish a protocol for WMNs, which contain the following components:

• An efficient anonymous routing protocol, which avoids network-wide flooding when establishing the routes, while ensuring both sender and receiver anonymity. All existing anonymous routing protocols targeted for general multi-hop wireless networks require network-wide flooding whenever a route needs to be established.

• An anonymous network access control protocol, which seamlessly integrated with the above anonymous routing protocol. This protocol prevents the WMNs from being abused by outsider attackers.

3.1 Network Model

A wireless network can operate in both the "Ad-hoc mode" where users are self managed and "Infrastructure mode" where an authority manages the network with some infrastructure such as fixed wireless routers, base station, access points etc. Ad-hoc network supports multi-hop where data packets may travel over multiple hops to reach its destination. Wireless Mesh Network is set of wireless mesh routers located at strategic points to provide overall network connectivity also provides flexibility of multi-hopping. They are dynamically self organized and self configured with the nodes in the network automatically establishing an ad hoc network and maintaining the mesh connectivity.

Wireless Mesh Networks (WMNs) represent a good solution to providing wireless Internet connectivity in a sizable geographic area; this new and promising paradigm allows for network deployment at a much lower cost than with classic Wi-Fi networks. In WMNs, it is possible to cover the same area (or even a larger one) with only one WHS and several wireless Transit Access Points (TAPs). The TAPs are not connected to the wired infrastructure and therefore rely on the WHS to relay their traffic.The network model proposed here is based on the assumption that the traffic is static or quasi-static. That it is reasonable since the traffic seen by the mesh routers is aggregated.

3.2 Basic Protocol Suite

Basic Protocol Suite used to achieve Privacy Against Passive attackers and other network users. This Protocol Consists 3 Parts:

1. Anonymous Local Key Establishment Protocol: Anonymous Local key Establishment Protocol is used to finding the sub sequent route Path. The user broadcasts a message within his neighborhood to initiate the key establishment protocol. Each of his neighborsreplies to the initiation message and derives session keys from the

message. For privacy protection, this protocol makes use of the group-signature technique to achieve anonymous authentication.

2. Node-to-Router path Finding and Registration protocol:Node-to-Router Path finding and Registration Protocol is used to establish the Router. This protocol is used to establish the route between mesh clients and mesh router, then register the client to the mesh router.

3. Anonymous Message Delivery Protocol: This Protocol is used to send a message anonymously delivered from source nodeto destination node.The delivery of the message consists of three steps

I.Uplink Routing (Node->router)

II. Router-Router routing(Router->Router)

III. Downlink Delivery(Router->Node)

3.3 Advanced Protocol Suite

Advanced Protocol Suite is used to achieve Privacy against Passive attackers andother network users. Additionally each user have a public/private key pair, Any User Knows other user‘s public key so that a secret key can be computed by a sender. The Advanced Protocol differs from Basic Protocol with respect to two aspects.

1. Anonymous User Registration.

User Registration is identity of a network user. Its avoids network-wide flooding by allowing each network user to register at mesh routers.

2.Onion-Routing-Based Router-Router Message Delivery.

It is used to find a simple source routing approach for the mesh router to Delivery Packets to each other.

3.4 Threat Model

A threat is an undesired event. A potential occurrence, often best described as an effect that might damage or compromise an asset or objective. Threat modeling is performed to identify when and where more effort should be applied. There are many possible vulnerabilities, threats, and exploits. Threat modeling is used to compromise the following Features:

- Sender/Receiver Anonymity: Receiver anonymity can also be compromised by the actual contents of the public key used to encrypt messages. If several senders share the same public key to encrypt messages to be sent for an anonymous receiver, then they can infer that they are in-deed sending to the same receiver. They can then aggregate the information they each have on that receiver to further compromise his anonymity. To achieve receiver anonymity a receiver must be able to create several truly anonymous identities that will allow for a sender to both encrypt and route messages to him.
- Relation Unlink ability Identify two communicating users even if they are not able to know their real identity.
- Session unlink ability: Link different communication sessions of the same users.

IV. PERFORMANCE EVALUATION

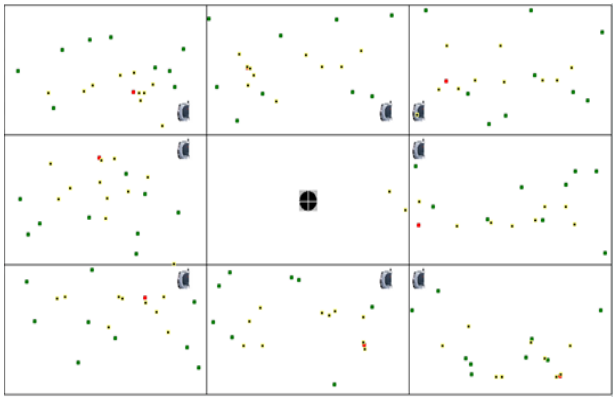

Figure 1: Anonymize the Nodes

In figure1, pictorially placed eight different mesh networks, place the mesh routers for the corresponding mesh, mesh routers would be placed on different blocks and the mesh router setup for the related mesh network would be implemented.Now to anonymize the users in the overall network following are the activities performed. Initially a public key is being established for the network which is known by all users in the network so that a secret key can be computed by a sender, followed by private keys for each mesh client is being set. Credentials of each node in a particular network would be shared with network head and network head receives it, similarly all the credentials are being received by base station respectively.

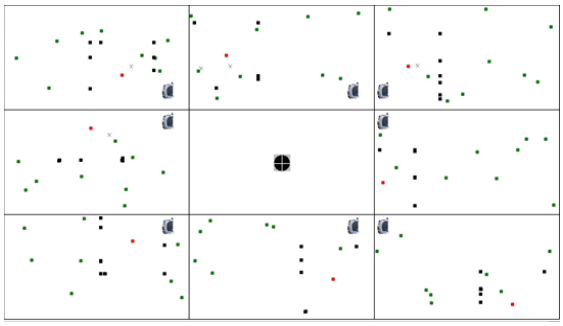

Figure 2: Credential Updation

In figure2, initiate credential sharing within the same cluster as described below:Not the entire network setup is established successfully, to test the data communication between clusters select the source cluster and source node along with destination cluster and destination node. Once the respective nodes and clusters are selected establish data communication between source node and destination node successfully.

V. CONCLUSION

In this paper, I had analyzed and reported some of the security and privacy issues in WMNs and proposed two protocol suite that mitigates the risks. Basic protocol suite ensures authentication within the group and ensuring that the data transfer route is established anonymously, the advanced protocol suite proposed enables shelter from passive attackers and other network users. The privacy preserving routing in WMNs has proposed two routing schemes to provide anonymity and unlink ability, as well as security, in WMNs. Both protocols have two stages: 1) the local session key establishment stage and 2) the anonymous routing-discovery stage. Relying

on the privacy protection of group signature schemes, the first stage anonymously constructs session keys, which are used in the second stage to protect privacy in routing discovery. In the first protocol, what a mobile user needs is only a group signature signing key, and privacy against outsiders is protected in this protocol. As in the first protocol, where mesh routers are still able to identify mobile users and track them, then the second protocol is designed to keep mobile users anonymous against mesh routers. Detailed security analysis and performance evaluation show that the proposed protocols are secure, privacy preserving, and efficient.

REFERENCES

[1] C. E. Perkins, Ad Hoc Networking. New York: Addison-Wesley, 2001.

[2] H. Yang, et al., "Security in Mobile Ad-Hoc Wireless Networks: Challenges and Solutions," IEEE Wireless Comm. Magazine, Feb 2004.

[3] Y. Challal, H. Bettahar and A. Bouabdallah, "A taxonomy of multicast data origin authentication, issues and solutions,"IEEE Comm. Surveys and Tutorials, Vol. 6, No. 3, pp. 34-57, 2004.

[4] A. Perrig, R. Canetti, D. Song, and D. Tygar, "Efficient Authentication and Signing of Multicast Streams over Lossy Channels." Proc. of the IEEE Symposium on Security and Privacy, Oakland, CA, May 2000.

[5] D. Balfanz, et al., "Talking to strangers: Authentication in ad-hoc wireless networks," Proc. of the Network and Distributed System Security Symposium (NDSS'02), San Diego, California, Feb 2002.

[6] R. Safavi-Naini and H. Wang, "Multi-receiver Authentication Codes: Models, Bounds, Constructions, and Extensions," Information and Computation, Vol. 151 No. 1-2, 25 pp. 148-172, May 1999.

[7] A. Perrig, "The BiBa One-time Signature and Broadcast Authentication Protocol," Proc. of the 8 th ACM Conf. on Computer and Communication Security, Philadelphia, PA, Nov 2001.

[8]. Adrian Perrig and D. Tygar, "Secure Broadcast Communication in wired and wireless networks". 2002: Kluwer.

[9]. B. Dahill, et al., "ARAN: A secure Routing Protocol for Ad Hoc Networks". 2002, UMASS Amherst.

[10]. P. Papadimitratos and Z. Haas. "Secure Routing for Mobile Ad Hoc Networks". in Proceedings of CNDS. 2002.