Trust-based Anonymity Framework for Wireless Mesh Networks

Muhammad Shoaib Siddiqui, Riaz Ahmed Shaikh, Choong Seon Hong
Dept. of Computer Engineering, Kyung Hee University, Global Campus, Korea
shoaib@networking.khu.ac.kr, riaz@oslab.khu.ac.kr, cshong@khu.ac.kr

Abstract — **Wireless Mesh Networks (WMN), this term was coined few years back in network research community. Due to its profound applicability, highly reliable connectivity, easy deployment, flexible interoperability with other networks drew much attention even within this short time. Although, lot of work is going on in this field but still issues like privacy and trust are left unattended. This paper address problems and solutions of these not well addressed issues i.e. ensuring privacy and anonymity in WMNs[1].**

Keywords — **Wireless Mesh Network, Privacy, Anonymity, Routing, Trust.**

1. Introduction

Wireless Mesh Networks (WMN) is a cost effective solution for network connectivity in areas where cabling is not a good solution or a fast deployment is required [1]. WMN [2] is a new and promising paradigm for providing wireless Internet connectivity in a geographic area. Due to its mesh characteristics, WMN provides high reliability and fault tolerance; with greater bandwidth and more reliable communication than conventional wireless networks. Although a lot of work is being done in routing issues of WMN, there is very little work being done in the fields of security and privacy. Open medium characteristics of the wireless links make WMN prone to attackers both from inside and outside of the network, and make it difficult to preserve both security and privacy in WMNs [3].

Privacy generally refers to the "ability to control the dissemination of information about oneself" [4]. More precisely privacy can be defined as "a state which can be lost, whether through the choice of the person in that state or through the action of another person" [5]. Privacy can be achieved through various different ways; one of the most common mechanisms used to achieve privacy is anonymity [6, 7]. The term anonymity generally refers to the condition in which an individual's identity remains undisclosed [8].

Preserving privacy in wireless mesh networks has more importance than the conventional network. As the neighboring nodes are responsible for routing the data from a sender to a receiving node, each node can look into the message; hence compromise the confidentiality of a message. Therefore, it should be assured that messages between the sender and receiver remain private and some kind of anonymity amongst the nodes is ensured. This paper provides some pioneering work in the field of privacy and anonymity in WMNs. In this paper we propose a Trust Based Anonymity (TBA) scheme for WMN.

The rest of the paper is organized as follows. In section 2, we start our discussion by first looking at the existing work done in the field of privacy in WMNs. Section 3, outlines the famous Onion routing, which is mostly used to provide privacy in networks. We identify the network model suitable for our proposal and potential adversaries along with the problem statement in section 4. In section 5, we proposed a trust based anonymity scheme that can be implemented in a scalable WMNs. Finally, we conclude our work and discuss the future enhancements in section 6.

2. Related Work

Current state-of-the-art research from privacy perspective in wireless mesh network is still in infancy state. According to authors' best of knowledge only two schemes [9] and [10] have been proposed so far for privacy in WMNs. In general, both schemes borrowed some design features from several existing works available in the literature. First we give a brief overview of both of the schemes emphasizing there assumptions, strengths and weakness and then we will describe our approach in detail.

Taojun Wu et. al. [10] have proposed a scheme that considers a new metric 'traffic entropy' to quantify the performance of a solution providing traffic privacy. It exploits redundancy in WMNs to hide information from an adversary by routing messages' fragments through multiple disjoint paths so that an adversary node cannot read the whole message. It also provides traffic confidentiality by dividing traffic spatially and temporally in a random way. But if the adversaries are working in a collaborative way or when an inside attacker colludes with an outside attacker; the proposed solution would fail to preserve privacy.

Xiaoxin Wu et al. [9] have proposed a solution to preserve privacy by using both cryptography and redundancy. The authors enhance the onion protocol, which provides anonymity in wired networks, to provide anonymity and privacy in WMNs. In this proposal, it is assumed that all information to and from the WMN is communicated through a centralized gateway. A locally deployed Public Key

[1] "This research was supported by the MKE under the ITRC support program supervised by the IITA"(IITA-2008-(C1090-0801-0016))
* Dr. CS Hong is corresponding author.

Infrastructure is deployed and maintained by that gateway. Also it is assumed that all the communication links are symmetric i.e. bi-directional and nodes communicate with each other using symmetric keys. The onion protocol makes the end nodes unlink-able but as the one of the communicating node is always the gateway, hence, the other end node is also traceable. The author proposed a logical ring topological implementation of the onion protocol to provide anonymity of the end node. In which all the transmission are started by the gateway router and also ended at the gateway router following a ring communication path.

3. Onion Routing

Onion routing [11] is the solution that uses some cryptographic and well known networking techniques to protect the privacy of internet communication against both the eavesdropping and traffic analysis. In Onion routing, setup begins when the initiator creates an onion. Each onion router along the route uses its private key to decrypt the entire onion that it receives. This operation exposes cryptographic control information for this onion router, the identity of next onion router in the path for this connection, and the embedded onion. The onion router pads the embedded onion to maintain it fixed sized and send it onwards. The final onion router in the path connects to a responder proxy, which will forward data to the remote application.

After the connection is established data can be send in both directions. The initiator's onion proxy receive data from application, breaks it into fixed size cells (128 bytes currently) and encrypt each cell multiple times – once for each onion router the connection traverse – using algorithms and keys specified in the onion. As a cell of data moves through anonymous connection, each onion router removes one layer of encryption, so the data emerges as a plain text from the final onion router in the path as shown in Figure 1. The responder proxy regroups the cell into data streams originally submitted by the application and forwards it to the destination.

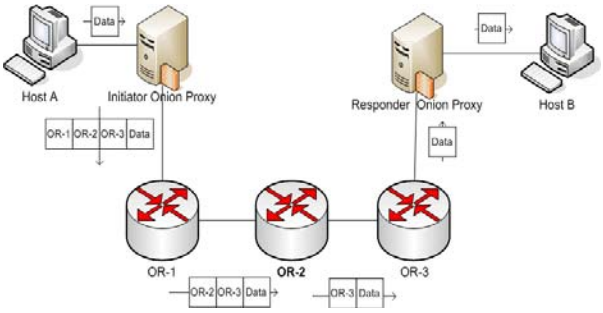

Figure 1. Data movement in Onion Routing

4. Problem Description

4.1 Network Model

We are assuming that there are multiple wireless mesh networks that are connected with each other via internet. Each wireless mesh network has its own gateway router that is a single entry and exit point through which each mesh users can communicate outside its own mesh network. We are also assuming that each gateway routers must knows, its network topology. Each gateway router and mesh user has a public key that is used for encrypting data. All mesh users can communicate with each other via wireless channel. We also assumed that all mesh users can communicate with each other through some multi-hop routing scheme. The basic wireless mesh network model is shown in Figure 2.

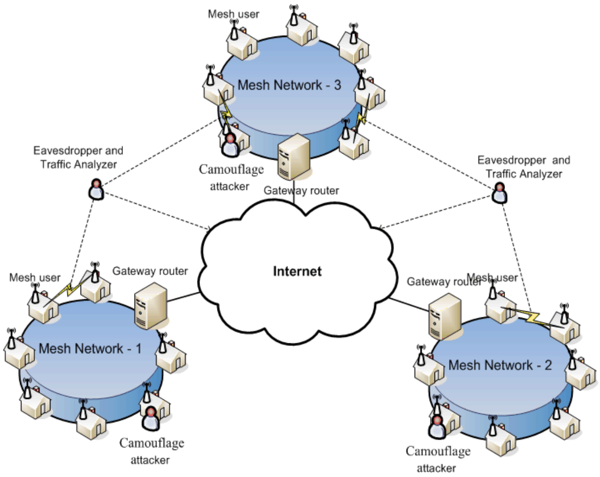

Figure 2. Wireless Mesh Network Model

4.2 Adversary Model

There are three common ways, through which privacy can be disclosed. One is by traffic analysis [12], second is by eavesdropping [13] and third is by camouflage [14].

- By traffic analysis, attacker can get access to the information like "who is talking to whom?"
- By eavesdropping attacker can get the information like "what nodes are talking about?" and
- By camouflaging, attacker can masquerade (via newly inserted node or via compromised node) as a normal node to magnetize the packets passes through it.

These three types of attacks can be performed by two types of attackers: one is "inside attacker" for example camouflage attacker and second is outsider attacker for example eavesdropper and traffic analyzer.

4.3 Problem Statement

In WMNs there are four kinds of privacy which we need to consider.

- Identity privacy: means no one can get any information about who is sending packets to whom? Only source and destination nodes can identity each other.

- ✧ Location privacy: means when an adversary captures the packet, he gets no clue to trace back the source or destination of a packet.
- ✧ Route privacy: means no nodes have any information about the location (in terms of physical distance or number of hops) about other nodes except for themselves, and
- ✧ Data or contents privacy.

Now problem here is to protect these four kinds of information against three different ways of privacy disclosure mechanism as discussed in adversary model section.

5. Trust-based Anonymity Scheme

Trust-based Anonymity Scheme (TBA) consists of two main components. One is called TBA Server and other is TBA Client. TBA server is installed on each mesh gateway router and TBA Client is installed on each mesh user. Let us first describe these two components first and then we will describe how both can achieve trust–based anonymity in WMNs.

5.1 TBA Server

TBA server is responsible for maintaining trust and anonymity between not only its own mesh users but also between multiple mesh networks. TBA server consists of three main components as shown in Figure 3.

1). Trust Manager
2). Virtual Mesh Manager and
3). Anonymity Manager

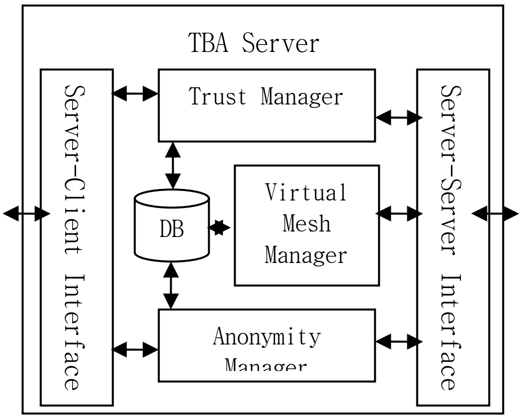

Figure 3. TBA Server Model

Trust Manager is responsible for calculating trust for not only mesh users but also for other mesh networks. Trust Manager will maintain the trust value of each mesh user in the network and for other mesh networks it will consider each other mesh networks as a single entity. For example if there are three other mesh networks of different sizes then TBA Server will maintain the single trust value irrespective of number of mesh users associated with respective mesh networks. This approach will give us two benefits one it reduces the computation cost, second it will consume less memory.

Trust value (T) is calculated, based on two parameters as discussed in [15]: Peer recommendation (PR) and other is past interactions (PI). Only one will considered at a time, for example if TBA server has no past interaction record then it will go for peer recommendation. Basic flow chart of calculating trust is shown in Figure 4. In order to calculate the trust value based on PI or PR various schemes available in the literature [15, 16]. We can use any one of them.

Virtual Mesh Network Manager is responsible for establishing virtual mesh network between various mesh networks that are attach to internet. This could be achieved by establishing tunnels between gateway routers as shown in Figure 5. Tunnels can be easily created with the help of IPSec protocol [17]. The basic objective of creating this virtual mesh network is to enable different mesh networks to communicate with each other in a secure and reliable manner by keeping their privacy intend.

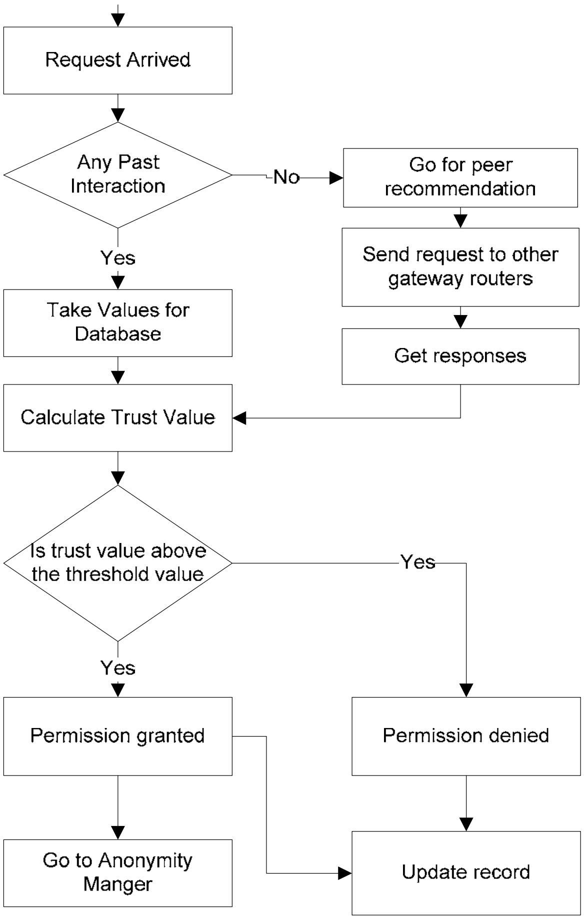

Figure 4. Flow-chart of TBA Trust Manager

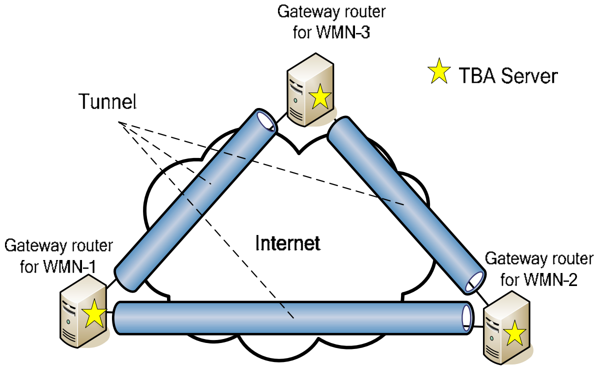

Figure 5. Virtual Mesh Network

Anonymity Manager is responsible for providing anonymity of identity, route, location and data as discussed in section 4.3. Anonymity manager works in following manner.

Step 1: Select '*j*' trustful nodes from the network of '*n*' nodes such that $0 < j <= n$.

Step 2: Construct a random path '*p*' that contain all trustful nodes including destination node. So the length '*l*' of path '*p*' is:

$l = j+1$ if $j<n$

$l = j$ if $j=n$

Step 3: Construct an onion packet. The layering of onion is based on the sequence of nodes in the path.

Step 4: That onion packet only traverse through the path *p*.

5.2 TBA Client

TBA client is installed on each mesh user. It is simplified versions of TBA Server only contain two main components: one is Trust manager and other is anonymity manager as shown in Figure 6. The functionality of trust manager and anonymity manager is same as discussed in section 5.1.

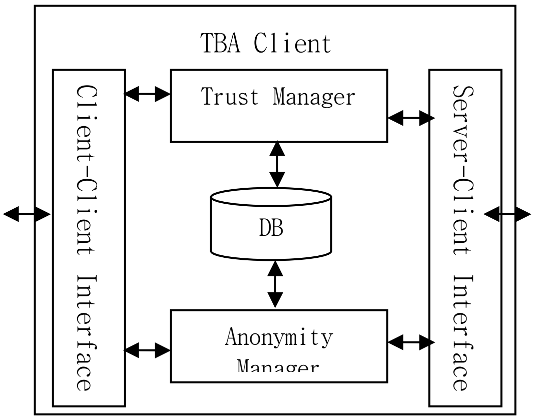

Figure 6. TBA Client Model

6. Conclusion and Future Work

Privacy and anonymity are key elements of any secure environment. This paper not only discussed some state-of-the art research of this field but also outlined the shortcomings of existing proposals and proposed a Trust Based Anonymity scheme for WMNs. This paper is our first step towards secure wireless mesh environment and provides a conceptual framework for it. We highlighted major components, their responsibilities and interactions, required to ensure privacy and anonymity in WMNs. In Future, we would clarify the implementation details of our scheme along with evaluation and comparison with existing frameworks.

REFERENCES

[1] J. Jangeun and M.L. Sichitiu, "The Nominal Capacity of Wireless Mesh Networks", In IEEE Wireless Communications, vol. 10(5), Oct. 2003, pp. 8-14

[2] K. Rayner, "Mesh wireless networking", Communications Engineer, vol. 1(5), Oct.-Nov. 2003, pp. 44-47

[3] Naouel Ben Salem and Jean-Pierre Hubaux, “Securing Wireless Mesh Networks”, IEEE Wireless Communication, vol. 13(2), April 2006, pp. 50 - 55

[4] Ross J. Anderson, “Security Engineering: A Guide to Building Dependable Distributed Systems”, Chapter 20, Publisher Wiley, Mar 2001

[5] Cedric Laurant, “Privacy and Human Rights 2003: An International Survey of Privacy Laws and Developments”, book, Publisher: EPIC and Privacy International, 1st edition 2003, http://www.privacyinternational.org/survey/phr2003/ overview.htm

[6] D. L. Chaum, “The dinning cryptographers problem: unconditional sender and recipient untraceability”, Journal of Cryptography 1(1), 1988, pp. 65-75

[7] Michael K. Reiter, and Aviel D. Rubin, “Crowds: Anonymity for Web Transactions”, ACM Transactions on Information and System Security, vol. 1(1), Jun 1998, pp. 66-92

[8] Microsoft Security Glossary, http://www.microsoft.com/ security/glossary.mspx, Updated: December 19, 2005

[9] Xiaoxin Wu, and Ninghui Li, “Achieving Privacy in Mesh Networks” , in proc. of SASN’06, oct 2006, Alexandria, Virginia, USA, pp. 13-22

[10] Taojun Wu, Yuan Xue and Yi Cui, “Preserving traffic privacy in wireless mesh networks”, in proc. of International Symposium on a World of Wireless, Mobile and Multimedia Networks, (WoWMoM 2006), Jun 2006, New York, USA, pp. 459-461

[11] M. Reed, P. Syverson, and D. Goldschlag. “Anonymous Connections and Onion Routing”, IEEE Journal on Selected Areas in Communications, vol. 16, no. 4, May 1998, pp. 482-494.

[12] Jing Deng, Richard Han, Shivakant Mishra, “Countermeasures Against Traffic Analysis Attacks in Wireless Sensor Networks”, Technical Report CU-CS-987-04, Computer Science Department, University of Colorado at Boulder, Dec 2004

[13] Djenouri, D. Khelladi, L. Badache, A.N., “A survey of security issues in mobile ad hoc and sensor networks”, IEEE Communications Surveys and Tutorials, vol. 7(4), 2005 , pp. 2-28

[14] John P. Walters, Zhengqiang Liang, Weisong Shi, and Vipin Chaudhary, “Wireless Sensor Networks Security: A Survey”, book chapter of Security in Distributed, Grid, and Pervasive Computing, Yang Xiao (Eds.), CRC Press, 2006

[15] Riaz Ahmed Shaikh, Hassan Jameel, Sungyoung Lee, Young Jae Song, and Saeed Rajput, “Trust Management Problem in Distributed Wireless Sensor Networks”, in proc. of 12th IEEE International Conference on Embedded Real Time Computing Systems and its Applications (RTCSA 2006), Sydney , Australia, Aug 2006, pp. 411-415

[16] Hassan Jameel, Le Xuan Hung, Umar Kalim, Ali Sajjad, Sungyoung Lee and Young-Koo Lee, “A Trust Model for Ubiquitous Systems based on Vectors of Trust Values”, in proc. of 3rd IEEE International workshop on Security in Storage, California, USA, Dec 2005, pp. 674-679

[17] S. Kent, and R. Atkinson, “Security Architecture for the Internet Protocol”, RFC 2401, Nov 1998