Volume 5, Issue 3, March 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Ticket- Based Anonymity and Traceability in Wireless Mesh Networks

Anil Kr. Panghal
CSE Deptt(HCTM)
Kaithal, Haryana, India

Sharda Rani
MCA Deptt(HCTM)
Kaithal, Haryana, India

Poonam
CSE Deptt, GJU University
Hisar, Haryana, India

Abstract -- A WMN is dynamically a self-organized and self-configured system with the nodes in the network automatically establishing and maintaining mesh connectivity among themselves. However, WMN is attractive to both the service providers and users and widespread due to its low investment feature and the wireless broadband services it supports, security issues inherent in mesh network or any wireless networks need be considered before deployment and proliferation of these networks, since it is unappealing to subscribers to obtain services without a security and privacy guarantee. It provides anonymity for the honest user's and trace the users who are misbehaving using other client's identification. Moreover, the approach to ensure the network access anonymity and location privacy, our pseudonym generation does not rely on a central authority, e.g., the broker, the domain authority.

Keywords -- Anonymity, Tickets, Traceability, WMN, Wireless.

I. INTRODUCTION

Wireless Mesh Networks (WMN) are gaining growing interest as a promising technology for ubiquitous high speed network access. The routing in wireless mesh networks is different from wired networks because of topology changes related to environmental fluctuations, limited bandwidth and battery life, partly unidirectional links, many redundant links, link quality. A WMN is dynamically a self-organized and self-configured system with the nodes in the network automatically establishing and maintaining mesh connectivity among themselves. However, WMN is attractive to both the service providers and users and widespread due to its low investment feature and the wireless broadband services it supports, security issues inherent in the mesh networks or any wireless networks need be considered before deployment and proliferation of these networks, since it is unappealing to subscribers to obtain services without a security and privacy guarantee. Anonymity and Traceability are considered as important concept in many payment based systems. Anonymity unlinks the user identities from his/her activities and also to prevent movement tracing by hiding location information in payment based systems. In unconditional anonymity, it is easier for any of the mesh network clients to misbehave and thus has not been traced. Even though there is pseudonym technique, to ensure that the network access anonymity and location privacy, it does not rely on central authority, who can derive the user's identity from his pseudonyms and illegally trace an honest user. Thus the concept of traceability is highly desirable in such systems.

This paper proposes a security architecture, that involves ticketing and blinding, resolve the conflicts between anonymity and traceability. Ticketing technique includes Ticket Issuance and Ticket Deposit, in which the tickets are issued, based on his/her misbehavior levels of the users, using Ticket Issuance Protocol, to do any processes and using Ticket Deposit Protocol, it is deposited. The borrowed Restrictive Partially Blind Signature technique , that acts as a backbone for our architecture. In this, with the help of Restrictiveness property, the user can get the signature by blinding his personal details and thus achieves anonymity. And with the help of Partial property, Trusted Authority (TA) can view some of the user detail in case of authentication. And, the dishonest users can be easily traced with the help of the Fraud Detection protocol.

II. RELATED WORK

Sensor networks are typically characterized by limited power supplies, small memory sizes, low bandwidth and limited energy. This leads to a very demanding environment to provide security issues. Majority of security issues have not been addressed and surveyed in .Universal pass model proposed for mesh networks, addressing countermeasures to wide range of attacks in WMNs. In the TA provides free Internet access but requires the clients (CLs) to be authorized and affiliated usres generally for a long term so that Ticket –based security architecture was developed which includes: Ticket issuance, Ticket deposit. Designing a ticket-based anonymity system with traceability property; bind of the ticket and pseudonym which guarantees anonymous access control (i.e., anonymously authenticating a user at the access point and simplified revocation process ,revocation of Tickets, adoption of the hierarchical identity-based cryptography (HIBC) for inter domain authentication avoiding domain parameter certification are illustrated in .Figure 1 explains the Ticket issuance and Deposit phases.

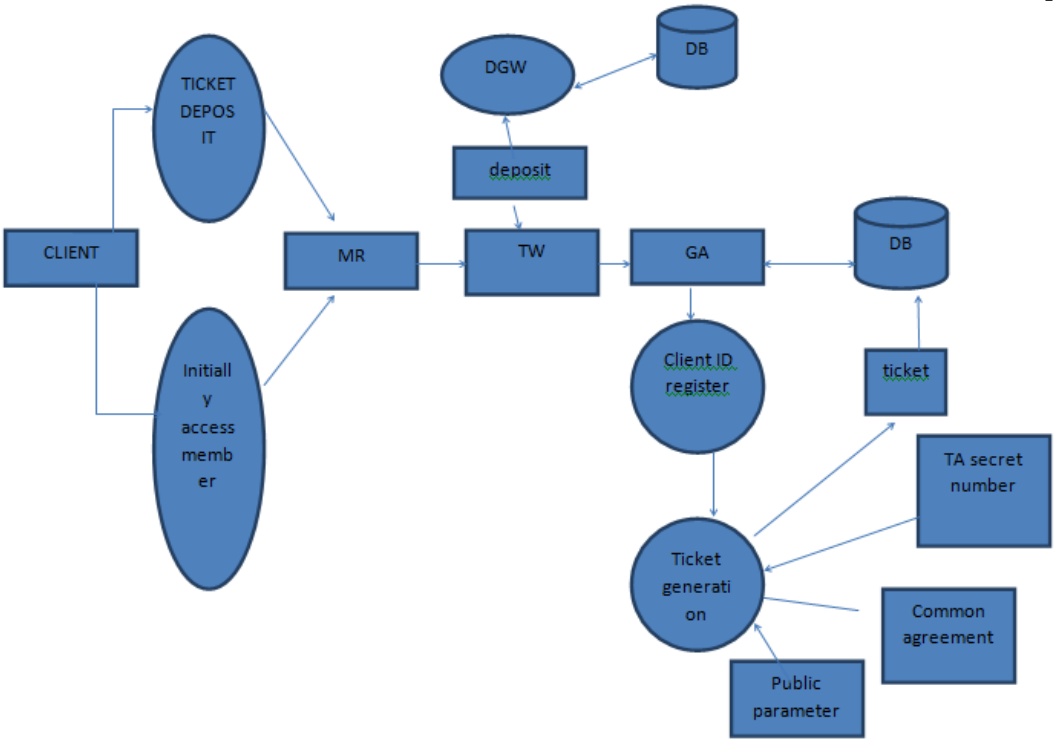

Fig1.Ticket Issuance and Ticket Deposit

Here Ticket issuance occurs when the user initially attempts to access the network or when all previously issued tickets are depleted. The user or client needs to reveal his real ID to the TA(Trusted Authority) in order to obtain a ticket since the TA has to ensure the authenticity of this client. After some process TA issues the batch of Tickets to MN (mobile Node). Ticket value is the total amount of traffic that the client is allowed to generate and receive before the expiry date of the ticket Misbehavior-Ticket reuse and multiple deposits. Ticket expiry date (validity period) after obtaining a valid ticket, the user may deposit it anytime the network service is desired before the ticket expires, using the ticket deposit protocol. Misbehavior is totally different from the noncompliant behavior.

III. EXISTING SYSTEM

In wireless communication systems, it is easier for a global observer to mount traffic analysis attacks by following the packet forwarding path than in the wired networks. Thus, routing anonymity is indispensable, which conceals the secret communication relationship of two parties by building an anonymous path between them. Nevertheless, unconditional anonymity may incur insider attacks since dishonest users are no longer traceable. Therefore, traceability is highly desirable such as in e-cash systems where it is used for detection and tracing double-spenders.

Disadvantages of Existing System: In the existing systems, there exists Conflicts between both the anonymity and traceability. The fundamental security requirements including authentication, data integrity, confidentiality and non-repudiation are not achieved in the existing systems.

IV. PROPOSED SYSTEM

In this paper, we propose a security architecture to ensure Unconditional anonymity for honest users and traceability of misbehaving users for Network authorities in wireless mesh networks (WMN). We are motivated by resolving the above security conflicts, namely anonymity and traceability concepts, in the emerging WMN communication systems. We have proposed the initial design of our security architecture, where the feasibility and the applicability of the architecture were not fully understood. As a result, we provide detailed efficiency analysis in terms of storage, communication, and computation in this paper to show that our proposed method is a practically viable solution to the application scenario of interest. We attacked Sun et al. scheme's traceability. Our analysis showed that trusted Authority (TA) cannot trace our system borrows the blind signature technique from the payment systems, and hence, can achieve the anonymity of unlinking user identities from activities, as well as the traceability of misbehaving users. Furthermore, the proposed pseudonym method renders user location information unexposed. Our proposed work differs from previous work in that WMNs have unique hierarchical topologies and rely heavily on wireless links, which have to be considered in the anonymity design. As a result, the original anonymity method for payment systems among bank, customer, and store cannot be directly applied. In addition to the anonymity method, other security issues such as authentication, key establishment, and revocation are critical in WMNs to ensure the correct application of the anonymity scheme. Moreover, although we employ the widely used pseudonym scheme to ensure network access anonymity and location privacy, our pseudonym generation does not rely on a central authority, e.g., the broker , the domain authority , the transportation authority or the manufacturer, and the trusted authority , who can derive the user's identity from his pseudonyms and illegally trace an honest user.

A. Wireless mesh networks

The wireless mesh backbone consists of mesh routers (MRs) and gateways (GWs) interconnected by using ordinary wireless links (shown as dotted curves). Mesh routers and the gateways serve as the access points of the WMN and the last resorts to the Internet, respectively. Each network domain, or trust domain (to be used interchangeably) is managed by a domain administrator that serves as a trusted authority the central server of a campus WMN.

B. Blind Signature

In general, a blind signature technique allows a receiver to obtain a signature on a message such that both the message and the resulting signature remain unknown to the signer. The formal definition of a blind signature scheme should bear the properties of verifiability, unlinkability, and unforgeability. Blind signature scheme, where the restrictiveness property is incorporated into the blind signature scheme such that the message being signed must contain the encoded information. As the name suggests, this property restricts the client in the blind signature scheme to embed some account-related secret information into what is being signed by the bank (otherwise, the signing will be unsuccessful) such that this secret can be recovered by the bank to identify a userif and only if he double-spends. The restrictiveness property is essentially the guarantee for traceability property in the restrictive blind signature systems.

C. Ticket Issuance

In order to maintain security of the network against attacks and the fairness among users, the home server manager may control the access of each client by issuing tickets based on the misbehavior history of the user, which reflects the server manager's confidence about the client to act properly. Ticket issuance occurs when theuser initially attempts to access the network or when all previously issued tickets are depleted. The client needs to reveal his/her real ID to the server manager in order to obtain a ticket since the server manager has to ensure the authenticity of this client.

D. Fraud Detection

Fraud is used interchangeably with misbehavior in this paper, which is essentially called an insider attack. Ticket reuse generally results from the client's inability to obtain the tickets from the TA when network access is desired, primarily due to the client's past misbehavior, which causes the server manager to constrain his ticket requests.

E. Fundamental security objectives

It is trivial to show that our security architecture satisfies the security requirements for data integrity, authentication and confidentiality, which follows directly from the employmentof the standard cryptographic primitives, message authentication code, and encryption, in our system. We are only left with the proof of non-repudiation in this category. A fraud can be repudiated only if the clientcan provide a different representation, he/she knows of message from what is derived by theserver manager. If the client has misbehaved, the representation he/she knows will be the sameas the one derived by the server Manager which ensures non-repudiation.

V. CONCLUSION

In this paper, we propose a security architecture mainly consisting of the User ticket-based protocols, in which Ticket was generated based on user profile (anonymity requirement) which resolves the conflicting security requirements of unconditional anonymity for honest users and traceability property of misbehaving users and the single Ticket is issued to every client so that storage overhead was reduced and it enhanced with Ticket renewal process. By utilizing the tickets based on the user profile, the proposed architecture is demonstrated to achieve desired security objectives and efficiency.

REFERENCES

[1] L. Zhou and Z. J. Haas, "Securing ad hoc networks," IEEE Network Magazine, vol.13, no.6, pp. 24–30, Dec. 1999.

[2] M. Raya and J-P.Hubaux, "Securing vehicular ad hoc networks," Journal of Computer Security, Special Issue on Security of Ad Hoc and Sensor Networks, vol. 15, no.1, pp. 39–68, 2007.

[3] N. B. Salem and J-P.Hubaux, "Securing wireless mesh networks,"IEEE Wireless Communications,vol. 13, no. 2, Apr. 2006.

[4] S. Brands, "Untraceable off-line cash in wallets with observers,"in Proc. CRYPTO'93, 13th Annual Int'l Cryptology Conf. on Advances in Cryptology, pp. 302–318, Aug. 1993.

[5] J. Sun, C. Zhang, and Y. Fang, "A security architecture achieving anonymity and traceability in wireless mesh networks," IEEE Conf. on Computer Communications (INFOCOM), pp. 1687–1695,Apr. 2008.

[6] X. Chen, F. Zhang, and S. Liu, "ID-based restrictive partially blind signatures and applications," Journal of Systems and Software, vol.80, no. 2, pp. 164–171, Feb. 2007.

[7] I.F. Akyildiz, X. Wang, and W. Wang, Wireless Mesh Networks: A Survey, Computer Networks, vol. 47, no. 4, pp. 445- 487, Mar. 2005.

[8] Y. Zhang and Y. Fang, ARSA: An Attack- Resilient Security Architecture for Multihop Wireless Mesh Networks, IEEE J. Selected Areas Comm., vol. 24, no. 10, pp. 1916- 1928, Oct. 2006.

