Efficient Security Architecture in WMN for finding Anonymity and Traceability

Roopa Mahadev
Department of Computer science and Engineering
East West Institute of technology, Bangalore, Karnataka, India.

Dr. Arun Biradar
Prof and Head
Department of Computer science and Engineering
East West Institute of technology, Bangalore, Karnataka, India.

Abstract- WIRELESS Mesh Network (WMN) is a promising technology and is expected to be widespread due to its low investment feature and the wireless broadband services it supports, attractive to both service providers and users. The nodes in the WMNs can configure automatically and re-configure dynamically to maintain the mesh connectivity. One of the fundamental challenges in WMNs is how to achieve Anonymity and traceability for mobile node. Anonymity has received increasing attention in the literature due to the users' awareness of their privacy nowadays. Anonymity provides protection for users to enjoy network services without being traced. In the existing architecture trusted authority issues the tickets to the client, it increases the client's storage overhead and adversary attacks. To avoid this, a new system in which the trusted authority provides single Ticket to the client during the ticket issuance protocol based on the user profile which is included in agreement and it includes the renewal field for deposited Ticket. It increases the client connectivity with its home trusted authority with considerable anonymity and traceability. Thorough analysis on security and efficiency is incorporated, demonstrating the feasibility and effectiveness of the proposed architecture.

Keywords – WMNs, Trusted Authority Anonymity, Traceability, Misbehavior, Revocation Renewal.

I. Introduction

In WMNs, nodes consists of mesh routers and mesh clients. Each node operates not only as a host but also as a router, forwarding packets on behalf of other nodes that may not be within direct wireless transmission range of their destinations. A WMN is dynamically self-organized and self-configured, with the nodes in the network automatically establishing and maintaining mesh connectivity among themselves (creating, in effect, an ad hoc network). This feature brings many advantages to WMNs such as low up-front cost, easy network maintenance, robustness, and reliable service coverage.

A wireless mesh network (WMN) is a communications network made up of radio nodes organized in a mesh topology. Wireless mesh networks often consist of mesh clients, mesh routers and gateways. The mesh clients are often laptops, cell phones and other wireless devices while the mesh routers forward traffic to and from the gateways. A mesh network is reliable and offers redundancy. When one node can no longer operate, the rest of the nodes can still communicate with each other, directly or through one or more intermediate nodes.

Anonymity and traceability have gained considerable research efforts in the literature which have focused on investigating anonymity in different context or application scenarios.. In WMNs the mobile node with high mobility can easily compromised by the adversary node in that network. So security is more important before the deployment of such networks. Nowadays user privacy is very important while accessing the network. For instance Anonymity is highly required for the honest user to unlink a user's identity to his or her specific activities in the network. And traceability is required for the misbehaved node in the network. Conditional anonymity is required for the misbehaved mobile node to trace its activity by Trusted Authority (or TA). Several solutions have been proposed in WMNs to address the privacy issues for mobile users.

II. Related Work

Sensor networks are typically characterized by limited power supplies, low bandwidth, small memory sizes and limited energy. This leads to a very demanding environment to provide security. Majority of security issues have not been addressed and surveyed in I.F. Akyildiz, X. Wang, and W. Wang [2].Universal pass model [3] proposed for WMNs, addressing countermeasures to wide range of attacks in WMNs. In J. Sun, Chi Zhang, Yanchao Zhang and

Yuguang Fang [1]the TA provides free Internet access but requires the clients (CLs) to be authorized and affiliated members generally for a long term so that Ticket –based security architecture was developed which includes Ticket issuance, Ticket deposit, .Design of 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 interdomain authentication avoiding domain parameter certification are illustrated in[1].

2.1 Ticket Issuance

In this paper, we are motivated by resolving the above security conflicts, namely anonymity and traceability, in the emerging WMN communication systems. Here Ticket issuance occurs when the client initially attempts to access the network or when all previously issued tickets are depleted. The 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 batch of Tickets to MN (mobile Node). The ticket generation algorithm[1], which can be any restrictive partially blind signature scheme in the literature, takes as input the client's and TA's secret numbers, the common agreement c, and some public parameters, and generates a valid ticket . A design issue to be pointed out is the commonly agreed information c negotiated at the beginning of the ticket generation algorithm. We define c as (ticket value, expiry date, misbehaviour,) , where Ticket Value- the total amount of traffic that the client is allowed to generate and receive before the expiry date of the ticket Misbehaviour-Ticket reuse and multiple deposits Expiry date-Ticket expiry date (validity period) After obtaining a valid ticket, the client may deposit it Anytime the network service is desired before the ticket expires, using the ticket deposit protocol . The DGW then creates a record for the deposited ticket as: record =(ticket,-,-, rem, log),where log field is created to record such noncompliant behavior [1].misbehavior is totally different from noncompliant behavior.

2.2. Limitations

Each client can get the series of Tickets during the Ticket issuance phase, so that client memory will be increased. And it place extra overhead in revocation process of unused Tickets.

Here Ticket value is assigned based on past misbehavior history of mobile node (client), there is no possible decision making function during the Ticket generation process for the mobile node who want to be a permanent user within that trust domain.

III. Proposed Algorithm

Ticket Generation based on user profile

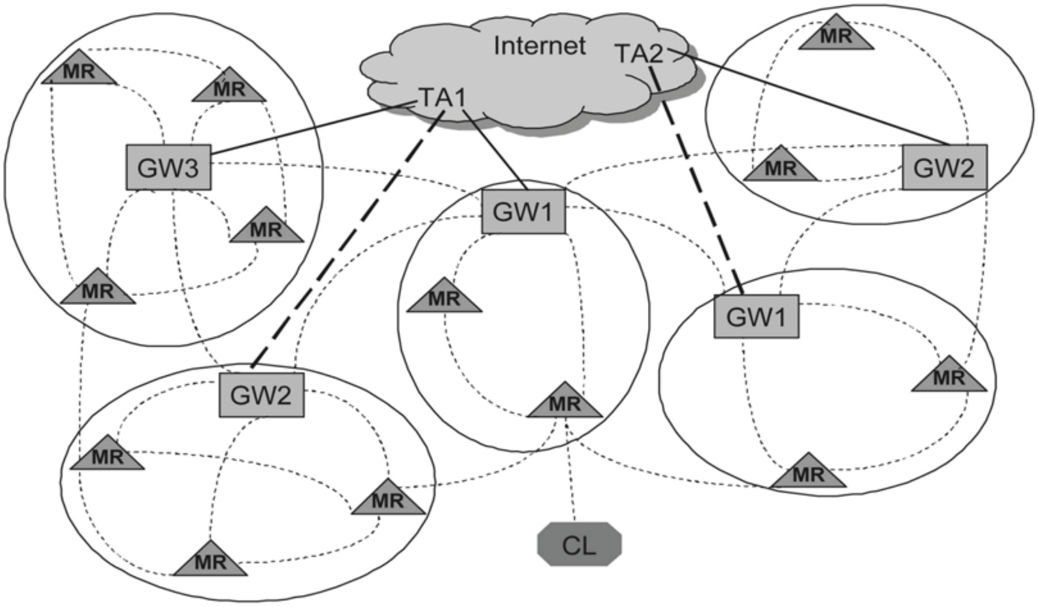

Fig 1: WMNs with Trusted Authority

In order to maintain security of the network against attacks and the fairness among clients, the home TA may control the access of each client by issuing tickets based on the misbehaviour history of the client, which reflects the TA's confidence about the client to act properly. Ticket issuance occurs when the client initially attempts to access the network [1][fig 1].

The proposed system includes the common agreement c(Val, exp , Mis , User Profile) for obtaining ticket from Trusted Authority(i.e. TA).

User Profile consists of 1) Long Term User with less anonymity 2) Short Term User with high anonymity based on this the client can get the suitable ticket value (Min or Max).restrictive Partially blind signature scheme is used for achieving anonymity for user [1] which borrows the blind signature technique [5][6][7] to achieve anonymity.ID based cryptography used for authentication purpose.

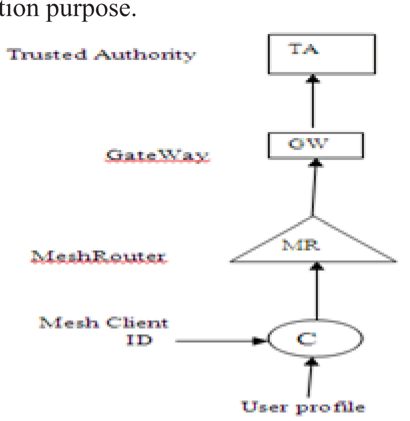

Fig 2.Profile based ticket Request

The mobile client can enter its ID and related information along with User profile to TA to get the Ticket [Fig 3].

3.1. Long Term User with less anonymity

If the client initially entered into the network, he or she can request Ticket from the TA to access the internet with free of cost .first the TA authenticates the client then it issues the Ticket to achieve anonymity and traceability of client. If the clients want to be a permanent user in particular domain, he or she uses this field. During the ticket generation protocol if the client sends this common agreement (c)

C (Val, exp, Mis, Long Term User)

Then the TA does the following steps

checks the past misbehavior history of the corresponding client

If (mis=0) then

checks the client anonymity requirement

Status

If (anonymity=not strict)

Then the TA will issue the Ticket with Higher value. if anonymity is not strictly required by the client, he can request tickets with higher values that can be used for longer time .This scheme is applied only for the new user and well behaved user in that network (mis=0).already visited client can also request the ticket with higher value, for this the same conditions are applied, in addition the TA checks the log field in the record generated by DGW.

3.2. Short Term User

The common agreement(c) , C(Val, exp, Mis, short Term user) is used to get the Ticket with lower value. Normally TA sets the lower value for the misbehaved clients to punish the clients. In addition if the mobile client having high mobility and it needs strict anonymity scheme, this field is used. The TA checks the user profile field in the C and assigns the value based on user requirements.

Note: The user profile can be varied for each time based on anonymity requirement of corresponding user.

IV. RENEWAL PROCESS AND EFFICIENCY ANALYSIS

4.1. deposited Ticket Renewal Process

After depositing a Ticket on a GW, the client can access the services until the Ticket expired, in the following cases the client can request Renewal process. The record generated by GW to the deposited ticked and forwarded to TA. This includes Renewal request.

Case 1: deposited ticket value is depleted before the expiry time.

Renewal request processing steps

```
1 .DGW informs the Client
(i.e. c(val=0,mis=0,exp=not expired))
2 If the Client wants renewal then
Renewal (ticket)
Else
Revocation (ticket)
3. DGW sends the request to TA
4. DGW and TA databases are updated
```

Case 2: The client wants to access the internet under the same ticket. i.e. the following condition
C (Val=0,mis=0,exp=expired)
Renewal process applicable only for the deposited Ticket (mis=0), and renewal process doesn't give fresh Ticket, it will increase the Ticket value for few seconds only .computation complexity increased for GWs in which renewal process is carried out.

4.2 .Efficiency Analysis

In existing a batch of Tickets is assigned to requested clients, but in this proposed model restriction applied for client requested message i.e. a client can get single Ticket during the ticket generation process. It decreases the client's storage overhead. The renewal process decreases the computation overhead of client. Revocation processes of unused tickets are eliminated. If the client wants another Ticket, it must initiate the revocation process for the old.

V. CONCLUSION

In this paper, I 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 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 user profile, the proposed architecture is demonstrated to achieve desired security objectives and efficiency.

REFERENCES

[1] IEEE transactions on Depentable and Secure computing vol 8, NO.2 march-april 2011 SAT: A Security Architecture Achieving Anonymity and Traceability in Wireless Mesh Networks Jinyuan Sun, Chi Zhang, Yanchao Zhang, and Yuguang Fang,

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

[3] 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.

[4] X. Chen, F. Zhang, and S. Liu, ―ID-Based Restrictive Partially Blind Signatures and Applications,‖ J. Systems and Software, vol. 80, no. 2, pp. 164-171, Feb. 2007.

[5] S. Brands, ―Untraceable Off-Line Cash in Wallets with Observers,‖Proc. 13th Ann. Int'l Cryptology Conf. Advances in Cyptology (CRYPTO '93), pp. 302-318, Aug. 1993.

[6] K. Wei, Y.R. Chen, A.J. Smith, and B. Vo, ―Whopay: A Scalableand Anonymous Payment System for Peer-to-Peer Environments,‖ Proc. IEEE Int'l Conf. Distributed Computing Systems (ICDCS), July 2006.

[7] D. Chaum, ―Blind Signatures for Untraceable Payments,‖ Advancesin Cryptology—Crypto '82, pp. 199-203, Springer-Verlag, 1982.

[8] J. Sun, C. Zhang, and Y. Fang, ―A Security Architecture Achieving Anonymity and Traceability in Wireless Mesh Networks,‖ Proc. IEEE INFOCOM, pp. 1687-1695, Apr. 2008.