Protection Architecture for Implementing Anonymity and Traceability in Wireless Mesh Network using Clustering Concept

CHATLA PRAVALLIKA
M.tech (cse)
Department of Computer Science & Engineering
AMR institute of technology, Mavala(v), Adilabad
Telangana State (India)

B. MANASA
M.tech (cse)
Assoc. Professor & HOD,
Computer Science & Engineering
AMR institute of technology, Mavala(v), Adilabad
Telangana State (India)

Abstract:
Wireless Mesh Network 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. However, security issues inherent in WMNs need be considered before the deployment and proliferation of these networks, since it is unappealing to subscribers to obtain services without security and privacy guarantees. For group formation multi-hop clustering algorithm namely "stable link clustering algorithm" was proposed which takes into account the long-term stability of links and neighbor nodes. Anonymity provides protection for users to enjoy network services without being traced. While anonymity related issues have been extensively studied in payment-based systems such as e-cash and peer-to-peer (P2P) systems, little effort has been devoted to wireless mesh networks (WMNs). On the other hand, the network authority requires conditional anonymity such that misbehaving entities in the network remain traceable. Security architecture to ensure unconditional anonymity for honest users and traceability of misbehaving users for network authorities in WMNs. The proposed architecture strives to resolve the conflicts between the anonymity and traceability objectives, in addition to guaranteeing fundamental security requirements including authentication, confidentiality, data integrity, and non- repudiation. Thorough analysis on security and efficiency is incorporated, demonstrating the feasibility and effectiveness of the proposed architecture.

Keywords: *Anonymity, Misbehavior, Psedonymn, Revocation, Traceability, Wireless mesh network (WMN)*

1. Introduction

A. Wireless mesh network

A wireless mesh network (WMN) [2] 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 WMN is shown in Figure 1.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. A Wireless mesh networks can be implemented

with various wireless technology including 802.11, 802.15, 802.16, cellular technologies or combinations of more than one type. Wireless mesh network can be seen as a special type of wireless ad-hoc network.

B. Cluster-Based Architecture

The process of organizing objects into groups whose members are similar in some way. The goal of clustering is to determine the intrinsic grouping in a set of related data. The cluster-based architecture consists in a set of unlabeled data. The cluster-based architecture consists of clusters. Each cluster should have one and only one Cluster Head (CH) which has the LMA functionality and complete knowledge about group membership and link state information in the cluster. A relay router connects two adjacent clusters. Access Routers (ARs), control heterogeneous radio access technologies and provide access to MNs. The backhaul between the CH and the ARs in the infrastructure can be wired or wireless. The MN, which attaches to the AR, can be connected through the backbone to all other ARs. The MN therefore can communicate with other mobile Correspondent Nodes (CNs) through ARs as well as with CNs on the Internet through CHs. This type of architecture is also applied in Wireless Mesh Networks. In the case of wireless backhaul, we have a Cluster Based WMN which can minimize the updating overhead during topology change due to mobility of mesh nodes.

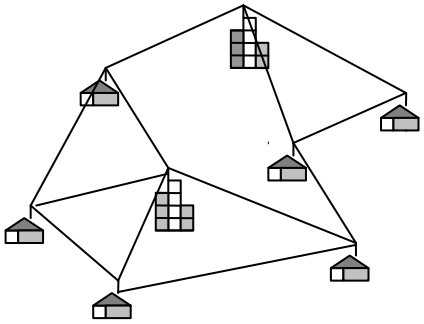

Fig. 1 Wireless Mesh Network

The cluster-based architecture consists in a set of unlabeled data. The cluster-based architecture consists of clusters. Each cluster should have one and only one Cluster Head (CH) which has the LMA functionality and complete knowledge about group membership and link state information in the cluster. A relay router connects two adjacent clusters. Access Routers (ARs), control heterogeneous radio access technologies and provide access to MNs. The backhaul between the CH and the ARs in the infrastructure can be wired or wireless. The MN, which attaches to the AR, can be connected through the backbone to all other ARs. The MN therefore can communicate with other mobile Correspondent Nodes (CNs) through ARs as well as with CNs on the Internet through CHs. This type of architecture is also applied in Wireless Mesh Networks. In the case of wireless backhaul, we have a Cluster Based WMN which can minimize the updating overhead during topology change due to mobility of mesh nodes.

If route optimization is considered, the traffic from one source MN to another destination MN should be able to pass through the relay router without passing through CHs.

2. Enhanced SLCA Based Security Architecture Stable Link Clustering Algorithm (SLCA)

The Stable Link Clustering algorithm [8] is based on a k- distance dominating set based clustering scheme with highest connectivity and several stability mechanisms [3]. Each node broadcasts a clustering message regularly every Cluster Message Interval seconds with a Time-To- Live of k hops. Based on the received clustering messages, each node calculates connection rating for every neighbor node. When a node receives a status message, the node calculates how many packets have been lost based on the status message packet sequence number. The connection rating is a penalty

function where a successfully received status message is awarded with one point and the loss of one or more packets is penalized with twice the number of lost packets. The Algorithm is shown in the table 1. The connection rating threshold is calculated based on the best connection rating in the neighbor. The idea is that only the nodes with the highest rating, with respect to the best node, are considered in the cluster head selection process.

Table: 1. SLCA Algorithm

Algorithm: 1

1: *CHcurr* ← 0 // current cluster head
2: *CHprev* ← 0// previous cluster head
3: *tprev* ← 0 // timestamp previous cluster head
4: *tloop* = 6∗ *Cluster Message Interval*
5: $a \geq 0$
6: **while** true **do**
7: Send and receive clustering messages
8: Calculate *rt*(*vj*) for all *vj* € *Nk*(*v*)
9: *deg*(*v*) ← $|N^r k\ (v)|$
10: **for** all *vj* € $N^r k\ (v)$ **do**
11: // candidate flap protection
12: **if** *deg*(*vj*) > *deg*(*CHcurr*) + *a* **then**
13: // candidate loop protection
14: **if** *vj* = *CHprev* **and** *tprev* + *tloop* > *now*() **then**
15: *tloop* ← *tloop* ∗ 2
16: **else** // Allow clusterhead change
17: *CHprev* ← *CHcurr*
18: *CHcurr* ← *vj* 19: *tprev* ← *now*() 20: **end if**
21: **end if**
22: **end for**
23: **end while**

3. Trust Model

The trust model is based on the trust relationships. The TA (Trusted Authority) is trusted within the WMN domain. There is no direct trust relationship between the client and the gateway/mesh router. A standard IBC [12],[13] is used for authentication and secure communications both at the backbone and during network access inside a trust domain (i.e.,intradomain). The client presents his ID upon registration at the TA, which assigns a private key associated with the client's ID. The client selects a unique account number computed by a randomly chosen secret number u1. The account number is stored with the client's ID at the TA. The TA also assigns an ID/private key pair to each gateway and mesh router in its trust domain before deployment. Advantages of this general trust relationship with the TA system from the direct authentication of the clients traveling among gateways/mesh routers in the same domain, which reduces network access latency and communication overhead that is expected to be overwhelming in future.

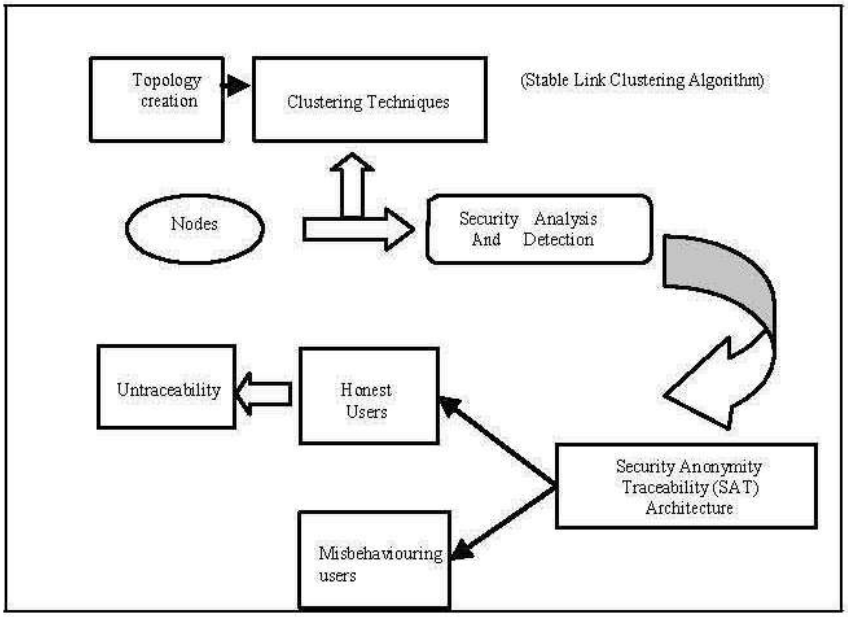

Figure 2. System Architecture

A. Architecture

WMNs, due to the large user population and high mobility. In accordance with the natural hierarchical architecture of the WMNs considered in this project, that adopt the hierarchical ID-based signature scheme (HIDS)[10]for interdomain authentication that occurs when a client affiliated with the home TA visits neighboring foreign TAs. Note that the basic HIDS is suitable when the level m of the signer in the hierarchical tree (HT) is close to the root at level 0, since the number of pairing operations and the size of the signature are determined by the signer's absolute location m. If m is relatively high the basic HIDS can be very inefficient in terms of computation and communication When a client roams to a foreign TA's domain (FTD) with a different master secret, to get the foreign TA's domain parameters certified by a trusted third party (TTP).The domain parameter certificate (DPC) issued by the TTP is then included in the inter domain authentication for verifying the authenticity of the domain parameters, which will later be utilized to verify the signature from the entities in FTD. Compared to that approach, the adopted HIDS scheme eliminates the requirement for the TTP and the DPCs. Furthermore, since that are concerned with the computation power of the clients, using the level assignment mentioned in the example above, the client needs to compute four pairings for verifying the signature from the access point (mesh router or gateway). In the client needs also to compute four pairings, two for DPC validation and two for verifying the signature from the access point if the efficient Hess's ID-based signature is used. Thus, the adopted HIDS scheme does not compromise the computation efficiency while increases the communication efficiency by the avoidance of DPCs.

4. SAT-Security Anonymity Traceability Ticket Based Architecture

The ticket-based security architecture consists of ticket issuance, ticket deposit, and fraud detection protocols.

A. Ticket Issuance

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 misbehavior 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 or when all previously issued tickets are depleted. The client needs to reveal his real ID to the TA in order to obtain a ticket since the TA has to ensure the authenticity of this client. Moreover, the TA should be unable to link the ticket it issued to the clients' real identities. The client thus employs some blinding technique to transform the ticket to be unlikable to a specific execution of the ticket generation algorithm, while maintaining the verifiability of the ticket. The ticket generation algorithm, 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.

B. Ticket Deposit

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 shown below. The scheme restricts the ticket to be deposited only once at the first encountered gateway that provides network access services to the client according to VAL before exp. The ticket is deemed valid if both the signature verification and the above equality check succeed.

The deposit gateway (DGW), where the ticket is initially deposited, will then generate a signature on the client's pseudonym, the DGW's ID, and the associated MISB and exp values extracted from c. The signature is required to be present in order for other access points in the trust domain to determine whether and where to forward the client's access requests, if the deposited ticket will be further used from other access points. This is the reason why the client is not allowed to change his pseudonym while still using a deposited ticket to which the pseudonym is associated, since the DGW will refuse to offer access services to the client if the present pseudonym mismatches the one recorded with the ticket. As a result, the ticket value needs to be set to a relatively small quantity in order to allow frequent update of the pseudonym if the client has high requirement on his anonymity. It will not place extra signaling overhead into the system since the TA can grant a batch of small-valued tickets during one single ticket issuance protocol.

C. Fraud Detection

Fraud is used interchangeably with misbehavior in this project, which is essentially an insider attack. Ticket reuse generally results from the client's inability to obtain tickets from the TA when network access is desired, primarily due to the client's past misbehavior, which causes the TA to constrain his ticket requests. Multiple -deposit can also be termed client coalition, which is beneficial when the coalescing parties are unauthorized users or clients with misbehavior history having difficulty in acquiring tickets from the TA. Note, however, that since a client is able to obtain multiple tickets in one ticket issuance protocol and self-generate multiple pseudonyms, he can distribute these pseudonym/ticket pairs to other clients without being traced as long as each ticket is deposited only once.

A possible remedy to this situation is to specify the non overlapping active period of a ticket instead of merely the expiry date/time such that each time, only one ticket can be valid. This approach, in general, requires synchronization. Another solution is to adopt the tamper-proof secure module so that a client cannot disclose his secrets to other parties since the secure module are assumed to be expensive and impractical to access or manipulate. This approach will eliminate the multiple deposit fraud but requires the deployment of secure modules.

5. Future Work

Anonymous routing serves as the enhancement to the user privacy, and we can provide multi hop uplink communications among clients in WMN. It is important for the user to be aware of his level of privacy. It makes a system more reliable and trustworthy for the user. Therefore it is important to analyze the problem how to measure the anonymity. However, since the anonymity level depends on the number of active users within the system the ticket based authenticated system informs the user about his protection level. Hence the level of the user's anonymous range was fixed by this scheme which entirely monitors the network. There exist certain Time to Live [TTL] value for particularly binded with the ticket's validity which indicate the time period for the service for that session. If the user exceeds the TTL value the system excludes the user from the network.

6. Conclusion

In this paper, we propose a SLCA which is based on the Highest Connectivity Criterion With topology stability optimizations. Security architecture mainly consisting of the ticket based protocols, which resolves the conflicting security requirements of unconditional anonymity for the honest users. By

using the above architecture the proposed work will be demonstrated to achieve desired security objectives and efficiency.

References

1. Akyildiz, F. X. Wang, and W. Wang, (2005). Wireless mesh networks: a survey, Comput. Netw., vol. 47, no. 4, pp. 445–487.
2. Boneh, D. and M. Franklin (2001). Identity-Based Encryption from the Weil Pairings Advances in Cryptology-Asiacrypt 2001, pp. 514-532, Springer-Verlag.
3. European Telecomm. e Standards Inst. (ETSI), GSM 2.09: Security Aspects, June 1993.
4. Gentry, C. and A. Silverberg, (2002). Hierarchical id-based crypto-graphy, Proc. ASIACRYPT, pp. 548–556.
5. Jinyuan sun, Chi Zhang,Yancho Zhang,Yuguang Fang, (2011). SAT: A Security Architecture achieving Anonymity and Traceability in wireless Mesh Network, IEEE transaction on dependable and secure computing
6. Juels, A., M. Luby, and R. Ostrovsky(1997). Security of blind digital signatures, Advances in Cryptology‖ - CRYPTO ’97, LNCS 1294, pp. 150-164, Springer-Verlag.
7. Kyasanur, P. and N. H. Vaidya, (2005). Selfish MAC layer misbehavior in wireless networks, IEEE Trans. Mobile Computing, vol. 4, no. 5, pp. 502–516.
8. Lim, H.W. (2006). On the Application of Identity-Based Cryptography in Grid Security, Ph.D. thesis, Univ. of London.
9. Martin Krebs, Andr´e Stein, M´onica Alejandra Lora, (2011). Topology Stability-based Clustering for Wireless Mesh Networks, IEEE Globecom.
10. Salem, N. B. and J-P. Hubaux (2006). Securing wireless mesh networks, IEEE Wireless communications, vol. 13, no. 2.
11. Wan, Z. K. Ren, B. Zhu, B. Preneel, and M. Gu, Anonymous User Communication for Privacy Protection in Wireless Metropolitan Mesh
12. Yong feng, Ming-yu fan, chang-ping liu,(2008). A New Privacy-enhanced Authentication Scheme for Wireless Mesh Networks, IEEE.
13. Yu, J. and P. Chong, (2005). A survey of clustering schemes for mobile ad hoc networks, Communications Surveys & Tutorials, IEEE, vol. 7, no. 1, pp. 32–48, Qtr.
14. Ze Wang, Yajuan Xing, Qi Wang, Wenju Liu, (2010). A Wireless Mesh network Secure Access method based on Identity-based Signature, IEEE
15. Zhiguo Wan, Kui Ren, Bo Zhu, Bart Preneel, and Ming Gu (2010). Anonymous User Communication for Privacy Protection in Wireless Metropolitan Mesh Networks, IEEE transactions on vehicular technology, vol. 59, no. 2.