ARCHITECTURE FOR ENSURING SECURITY REQUIRMENTS IN WIRELESS MESH NETWORKS

Chirla Vineela[1], M. Rambhupal[2]

ADITYA ENGINEERING COLLEGE, JNTU KAKINADA, Department of Information Technology, Surampalem, AP, India
[1]vineela.chirla@gmail.com, **[2]bhupal.ram@gmail.com**

Abstract

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. 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.

Here, we propose a security architecture to ensure unconditional anonymity for honest users and traceability of misbehaving users for network authorities in WMNs. [1]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 no repudiation. Thorough analysis on security and efficiency is incorporated, demonstrating the feasibility and effectiveness of the proposed architecture.

***Keywords**: Anonymity, Traceability, Wireless mesh networks, Privacy, Misbehaving users, e-cash systems, Confidential communication*

----------***----------

1. INTRODUCTION

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. However, security issues inherent in WMNs or any wireless networks 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.[2] Wireless security has been the hot topic in the literature for various network technologies such as cellular networks, wireless local area networks (WLANs), wireless sensor networks, mobile ad hoc networks (MANETs), and vehicular ad hoc networks (VANETs). [3]Anonymity and privacy issues have gained considerable research efforts in the literature, which have focused on investigating anonymity in different context or application scenarios. One requirement for anonymity is to unlink

a user's identity to his or her specific activities, such as the anonymity fulfilled in the untraceable e-cash systems and the P2P payment systems, where the payments cannot be linked to the identity of a payer by the bank or broker. Anonymity is also required to hide the location information of a user to prevent movement tracing, as is important in mobile networks and VANETs. In wireless communication systems, it is easier for a global observer to mount traffic analysis attacks by following the packet-forwarding path than in wired networks. Thus, routing anonymity is indispensable, which conceals the confidential communication relationship of two parties by building an anonymous path between them. Nevertheless, unconditional anonymity may incur insider attacks since misbehaving users are no longer traceable. Therefore, traceability is highly desirable such as in e-cash systems, where it is used for detecting and tracing double-spenders.

1.1. 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 wired networks. Thus, routing anonymity is indispensable, which conceals the confidential communication relationship of two parties by building an anonymous path between them. Nevertheless, unconditional anonymity may incur insider attacks since misbehaving users

are no longer traceable. Therefore, traceability is highly desirable such as in e-cash systems where it is used for detecting and tracing double-spenders.

1.2. Proposed System

We are motivated by resolving the above security conflicts, namely anonymity and traceability, in the emerging WMN communication systems. We have proposed the initial design of our security architecture, where the feasibility and 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 SAT is a practically viable solution to the application scenario of interest. Our system borrows the blind signature technique from 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 technique renders user location information unexposed.

1.3 Advantage

Our 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 scheme for payment systems among bank, customer, and store cannot be directly applied. In addition to the anonymity scheme, 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 approach 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. Our system is not intended for achieving routing anonymity, which can be incorporated as an enhancement.

2. PROBLEM DEFINITION

A large number of studies on multi-hop wireless networks have been devoted to system stability while maximizing metrics like throughput or utility. These metrics measure the performance of a system over a long time-scale. For a large class of applications such as video or voice over IP, embedded network control and for system design; metrics like delay are of prime importance. [4]The delay performance of wireless networks, however, has largely been an open problem. This problem is notoriously difficult even in the context of wireline networks, primarily because of the complex interactions in the network (e.g., superposition, routing, departure, etc.) that make its analysis amenable only in very special cases like the product form networks. The problem is further exacerbated by the mutual interference inherent in wireless networks which, complicates both the scheduling mechanisms and their analysis. Some novel analytical techniques to compute useful lower bound and delay estimates for wireless networks with single hop traffic were developed.

We analyze a multi-hop wireless network with multiple source-destination pairs, given routing and traffic information. [5]Each source injects packets in the network, which traverses through the network until it reaches the destination. For example, a multi-hop wireless network with three flows. The exogenous arrival processes correspond to the number of packets injected in the system at time . [6]A packet is queued at each node in its path where it waits for an opportunity to be transmitted. Since the transmission medium is shared, concurrent transmissions can interfere with each others' transmissions. The set of links that do not cause interference with each other can be scheduled simultaneously, and we call them activation vectors (matching's). We do not impose any a priori restriction on the set of allowed activation vectors, i.e., they can characterize any combinatorial interference model. For example, in a K-hop interference model, the links scheduled simultaneously are separated by at least K hops. each link has unit capacity; i.e., at most one packet can be transmitted in a slot. For the above example, we assume a 1-hop interference model. The delay performance of any scheduling policy is primarily limited by the interference, which causes many bottlenecks to be formed in the network. We demonstrated the use of exclusive sets for deriving lower bounds on delay for a wireless network with single hop traffic.

We define the major aspects of concern which are Anonymity (Untraceability): the anonymity of a legitimate client refers to the untraceability of the client's network access activities. The client is said to be anonymous if the TA, the gateway, and even the collusion of the two cannot link the client's network access activities to his real identity. Traceability: a legitimate client is said to be traceable if the TA is able to link the client's network access activities to the client's real identity if and only if the client misbehaves, i.e., one or both of the following occurs: ticket reuse and multiple deposit.

3. COMPONENTS

3.1. Wireless mesh networks (WMNs)

The wireless mesh backbone consists of mesh routers (MRs) and gateways (GWs) interconnected by ordinary wireless links (shown as dotted curves). [7]Mesh routers and gateways serve

as the access points of the WMN and the last resorts to the Internet, respectively. Each WMN 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. The TA and associated gateways are connected by high-speed wired or wireless links, displayed as solid and bold dashed lines, respectively. TAs and gateways are assumed to be capable of handling computationally intensive tasks. In addition, they are assumed to be protected in private places and cannot be easily compromised due to their important roles in the WMN. The WMNs of interest here are those where the TA provides free Internet access but requires the clients (CLs) to be authorized and affiliated members generally for a long term, as the employees or students in the case of enterprise and hospital WMNs or campus WMNs. Such individual WMN domains can be building blocks of an even larger metropolitan WMN domain.

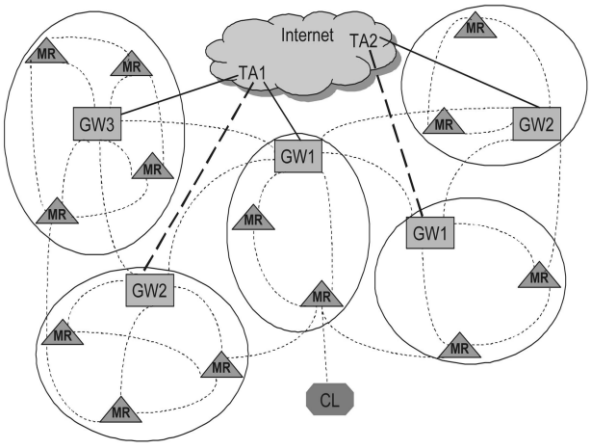

Figure 1. Typical Wireless Mesh Network topology

3.1.1 Blind Signature

In general, a blind signature scheme allows a receiver to obtain a signature on a message such that both the message and the resulting signature remain unknown to the signer. We refer the readers for a formal definition of a blind signature scheme, which should bear the properties of verifiability, unlink ability, and unforgeability. It is a scheme, where the restrictiveness property is incorporated into the blind signature scheme such that the message being signed must contain encoded information. As the name suggests, this property restricts the user 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 user if and only if he double-spends. The restrictiveness property is essentially the guarantee for traceability in the restrictive blind signature systems.

3.1.2 Ticket Issuance

In order to maintain security of the network against attacks and the fairness among clients, the home server manager may control the access of each client by issuing tickets based on the misbehavior history of the client, which reflects the server manager'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 server manager in order to obtain a ticket since the server manager 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 un linkable to a specific execution of the ticket generation algorithm (the core of ticket issuance protocol), 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. Partially blind signatures alone allow the blind signature to carry explicit information on commonly agreed terms (i.e., ticket value, expiry date, misbehaviour, etc.) which remains publicly visible regardless of the blinding process. Restrictive blind signatures place restrictions on the client's selection of messages being signed which contain encoded identity information (in TN) instead of completely random numbers, allowing the TA to recover the client's identity if and only if misbehavior is detected. As a result, the anonymity of an honest client is unconditionally ensured.

3.1.3 Fraud Detection

Fraud is used interchangeably with misbehavior in this paper, 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 server manager 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 misbehaviour 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 is 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. In the following discussion, we will still consider multiple deposit as a possible type of fraud (e.g., in case that secure modules are unavailable). These two types of fraud share a common feature, that is, a same ticket (depleted or valid) is deposited more than once such that our one-time deposit rule is violated. This is where the restrictiveness of the blind signature algorithm takes effect on revealing the real identity of the misbehaving client. Specifically, when the TA detects duplicate deposits using the ticket records reported by gateways, the TA will have the view of at least two different challenges from gateways and two corresponding sets of responses from the same client. By solving the equation sets below based on these challenges and responses, the TA is able to obtain the identity information encoded in the message, and hence, the real identity of the misbehaving client.

3.1.4 Fundamental security objectives

It is trivial to show that our security architecture satisfies the security requirements for authentication, data integrity, and confidentiality, which follows directly from the employment of 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 client can provide a different representation, he knows of message from what is derived by the server manager. If the client has misbehaved, the representation he knows will be the same as the one derived by the server Manager that ensures non repudiation.

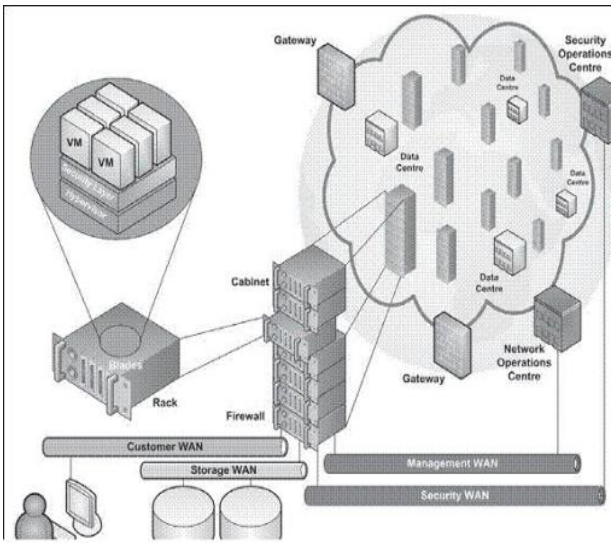

Figure 2. Architecture

4. CONCLUSION

We propose SAT, a security architecture mainly consisting of the ticket-based protocols, which resolves the conflicting security requirements of unconditional anonymity for honest users and traceability of misbehaving users. By utilizing the tickets, self-generated pseudonyms, and the hierarchical identity-based cryptography, the proposed architecture is demonstrated to achieve desired security objectives and efficiency.

Future Enhancement In the WMNs considered here, the uplink from the client to the mesh router may rely on multihop communications. Peer clients act as relaying nodes to forward each other's traffic to the mesh router, which forms a P2P network. [13]The notorious problem common in P2P communication systems is the free-riding, where some peers take advantage of the system by providing little or no service to other peers or by leaving the system immediately after the service needs are satisfied. Peer cooperation is thus the fundamental requirement for P2P systems to operate properly. Since peers are assumed to be selfish, incentive mechanisms become essential to promote peer cooperation in terms of both cooperativeness and availability. Typical incentive mechanisms for promoting cooperativeness include reputation and payment-based approaches. In the reputation-based systems, peers are punished or rewarded based on the observed behavior. However, low availability remains an unobservable behavior in such systems, which hinders the feasibility of the reputation-based mechanism in improving peer availability. By contrast, the payment-based approach provides sufficient incentives for enhancing both cooperativeness and availability, and thus, is ideal to be employed in multihop uplink communications among peer clients in our WMN system.

REFERENCES

[1] H. Balakrishnan, C. Barrett, V. Kumar, M. Marathe, and S. Thite. The distance-2 matching problem and its relationship to the maclayer capacity of ad hoc networks. IEEE Journal on Selected Area in Communications, 22, 2004.
[2] L. Bui, R. Srikant, and A. L. Stolyar. Novel architectures and algorithms for delay reduction in backpressure scheduling and routing. INFOCOM Mini-Conference, 2009.
[3] P. Chaporkar, K. Kar, and S. Sarkar. Throughput guarantees through maximal scheduling in wireless networks. In 43rd Annual Allerton Conference on Communication, Control, and Computing, 2005.
[4] J. G. Dai and W. Lin. Maximum pressure policies in stochastic processing networks. Operations Research, 53:197–218, 2005.

[5] J. G. Dai and W. Lin. Asymptotic optimality of maximum pressure policies in stochastic processing networks. Preprint, October 2007.
[6] H. Dupuis and B. Hajek. A simple formula for mean multiplexing delay for independent regenerative sources. Queueing Systems Theory and Applications, 16:195–239, 1994.
[7] A. Feldmann, N. Kammenhuber, O. Maennel, B. Maggs, R. D. Prisco, and R. Sundaram. A methodology for estimating interdomain web traffic demand. In IMC, 2004.
[8] L. Georgiadis, M. J. Neely, and L. Tassiulas. Resource Allocation and Cross-Layer Control in Wireless Networks, Foundations and Trends in Networking, volume 1. Now Publishers, 2006.
[9] G. R. Gupta. Delay Efficient Control Policies for Wireless Networks. Ph.D. Dissertation, Purdue University, 2009.
[10] G. R. Gupta, S. Sanghavi, and N. B. Shroff. Node weighted scheduling. SIGMETRICS-Performance'09, June 2009.
[11] G. R. Gupta, S. Sanghavi, and N. B. Shroff. Workload optimality in switches without arrivals. Mathematical performance Modeling and Analysis Workshop, June 2009.
[12] G. R. Gupta and N. B. Shroff. Delay analysis for wireless networks with single hop traffic and general interference constraints. IEEE Transactions on Networking, 18:393 – 405, April 2010.
[13] S. Jagabathula and D. Shah. Optimal delay scheduling in networks with arbitrary constraints. In ACM SIGMETRIC/Performance, June 2008.
[14] K. Jain, J. Padhye, V. Padmanabhan, and L. Qiu. Impact of interference on multi-hop wireless network performance. In MOBICOM, 2003.

BIOGRAPHIES

Chirla Vineela
II year MTech
Dept of Information Technology
Aditya Engineering College
Surampalem, Andhra Pradesh, India
vineela.chirla@gmail.com

M.Rambhupal
Asst Professor
Dept of Computer Science Engg
Aditya Engineering College
Surampalem, Andhra Pradesh, India
bhupal.ram@gmail.com