International Journal of Modern Engineering Research (IJMER)
www.ijmer.com Vol.2, Issue.5, Sep-Oct. 2012 pp-3973-3976 ISSN: 2249-6645

A Ticket Based Architecture for Providing Anonymity and Traceability in Wireless Mesh Network

S.Parvaiz[1], V. Sreenatha Sarma[2]
[1, 2] *(M. tech, Department of CSE, ASCET, GUDUR,*

ABSTRACT: *A wireless mesh is a communication network made up of radio nodes organized in a mesh topology. A wireless mesh network help users to stay online anywhere, anytime for an unlimited time and it provide high security.In this paper we come across two issues one is anonymity and other is traceability. Anonymity provides protection for users to enjoy network services without being traced. Now a day's Anonymity has received increasing attention in the literature due to the users' awareness of their privacy. 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). The network authority requires conditional anonymity such that misbehaving entities in the network remain traceable.so in order to provide high network security we provide a secure architecture to ensure unconditional anonymity for honest users and traceability of misbehaving users for network authorities in WMNs. This architecture strives to resolve the conflicts between the anonymity and traceability objectives.Finally the architecture guaranteeing fundamental security requirements such as authentication, confidentiality, data integrity, and norepudiation.*

I. INTRODUCTION

Traceability is the ability to map events in cyberspace, particularly on the Internet, back to real-world instigators, often with a view to holding them accountable for their actions. Anonymity is present when traceability fails. Failures of traceability, with consequent unintentional anonymity, have continued as the technology has changed. The underlying reason for this continuing failure is a lack of economic incentives for improvement. The lack of traceability at the edges is further illustrated by a new method of stealing another person's identity on an Ethernet Local Area Network that existing tools and procedures would entirely fail to detect. Anonymity and privacy issues have gained considerable research efforts, 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. 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. 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. Wireless Mesh Networks (WMNs) have become the focus of much research since they allow for increased coverage while retaining the attractive features of low cost and easy deployment. WMNs have been identified as key technology to enhance and compliment existing network installations as well as provide access where traditional technology is not available or too costly in install. A WMN is made up of mesh routers (MRs), which have limited or no mobility, and mesh clients (MCs) which are often fully mobile. The mesh routers form the backbone of the network allowing the clients to have access to the network through the backbone. We propose an algorithm for fair scheduling in WMNs with multiple gateways. We also propose another algorithm for scheduling which places more emphasis on throughput while retaining a basic level of throughput called mixed-bias. This technique biases against characteristics of the network which are detrimental to performance, fairness, or both. Many protocols currently implemented for WMNs have evolved from traditional single-hop wireless local area networks (WLAN) and mobile ad-hoc networks (MANET). However, both of these networks have characteristics which make them very different from WMNs. While WLANs have relatively static topologies, MANETs on the other hand are fully mobile.

Therefore, using protocols designed solely for either of these networks alone does not take advantage of some of the most advantageous features of WMNs. In MANETs all nodes are routers and suffer from limited power and bandwidth. In a WMN the MRs have greater resources available than the MCs which is a property that may be exploited. Although a lot of research efforts have been made to address these problems and some new specialized algorithms have been proposed specifically for WMNs, there are still many challenges in the area. Many of the existing solutions make many assumptions that can be relaxed to allow for a more general approach to be taken.

Here, 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. 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.

II. System Architecture

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. The delay performance of wireless networks, however, has largely been an open problem. This problem is notoriously difficult even in the context of wire line 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. 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. 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* (matchings). 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 the purpose of deriving lower bounds on delay for a wireless network with single hop traffic.

A. Proposed approach

All projects are feasible when provided with unlimited resources and infinite time! Unfortunately, the development of computer-based system or product is more likely plagued by a scarcity of resources and difficult delivery dates. It is both necessary and prudent to evaluate the feasibility of a project at the earliest possible time. Months or years of effort, thousands or millions of dollars, and untold professional embarrassment can be averted if an ill-conceived system is recognized early in the definition phase. Feasibility and risk analysis are related in many ways. If project risk is great the feasibility of producing quality software is reduced. During product engineering, however, we concentrate our attention on four primary areas of interest.

B. Technical Feasibility

This application in going to be used in an Internet environment called www (World Wide Web). So, it is necessary to use a technology that is capable of providing the networking facility to the application. This application as also able to work on distributed environment. Application on developed with J2EE (Java 2 Enterprise Edition platform) Technology. One major advantage in application is platform neutral. We can deploy and used it in any operating system. GUI is developed using HTML to capture the information from the customer. HTML is used to display the content on the browser. It uses TCP/IP protocol. It is an interpreted language. It is very easy to develop a page/document using HTML some RAD (Rapid Application Development) tools are provided to quickly design/develop our application. So many objects such as button, text fields, and text area etc are provided to capture the information from the customer.

C. Economical Feasibility

The economical issues usually arise during the economical feasibility stage are whether the system will be used if it is developed and implemented, whether the financial benefits are equal are exceeds the costs. The cost for developing the project will include cost conducts full system investigation, cost of hardware and software for the class of being considered, the benefits in the form of reduced costs or fewer costly errors. The project is economically feasible if it is developed and installed. It reduces the work load. Keep the class of application in the view, the cost of hardware and software is considered to be economically feasible.

D. Operational Feasibility

In our application front end is developed using GUI. So it is very easy to the customer to enter the necessary information. But customer has some knowledge

on using web applications before going to use our application.

E. Social Feasibility

It is a determination of whether the people will accept a proposed project or not.

F. Management Feasibility

It determines whether the proposed project will be acceptable to the management.

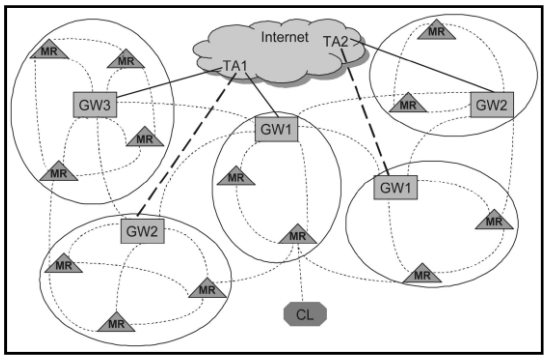
G. Legal Feasibility

These concerns about the legalities are satisfied.

H. Time Feasibility

It determines whether a proposed project can be implemented fully within stipulated time. We strongly feel that the proposed system is feasible in all respects.

Network Architecture:



The wireless mesh backbone consists of mesh routers (MRs) and gateways (GWs) interconnected by ordinary wireless links (shown as dotted curves). 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 (TA), e.g., the central server of a campus WMN. 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.

III. TECHNIQUES OF ARCHITECTURE

A. 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). 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.

B. 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, 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 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.

C. 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.

D. 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.

E. 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 nonrepudiation 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 which ensures nonrepudiation. Ad hoc networks inherit some of the traditional problems of wireless communication and wireless networking:

I. The wireless medium does not have proper boundaries outside of which nodes are known to be unable to receive network frames.

II.The wireless channel is weak, unreliable, and unprotected from outside signals, which may cause lots of problems to the nodes in the network.

III.The wireless channel has time-varying and asymmetric propagation properties.

IV.Hidden-node and exposed-node problems may occur.

IV. Result

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. 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. So, Finally the architecture guaranteeing fundamental security requirements such as authentication, confidentiality, data integrity, and norepudiation.

V. 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. 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. 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] European Telecomm. Standards Inst. (ETSI), "GSM 2.09: Security Aspects," June 1993.
[2] P. Kyasanur and N.H. Vaidya, "Selfish MAC Layer Misbehavior in Wireless Networks," IEEE Trans. Mobile Computing, vol. 4, no. 5, pp. 502-516, Sept. 2005.
[3] A. Perrig, J. Stankovic, and D. Wagner, "Security in Wireless Sensor Networks," Comm. ACM, vol. 47, no. 6, pp. 53-57, 2004.
[4] S. Zhu, S. Setia, and S. Jajodia, "LEAP+: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks,"ACM Trans. Sensor Networks, vol. 2, no. 4, pp. 500-528, Nov. 2006.
[5] W. Lou and Y. Fang, A Survey on Wireless Security in Mobile Ad Hoc Networks: Challenges and Possible Solutions, X. Chen, X. Huang, and D.-Z. Du, eds., Kluwer Academic Publishers/Springer, 2004.
[6] L. Zhou and Z.J. Haas, "Securing Ad Hoc Networks," IEEE Network Magazine, vol. 13, no. 6, pp. 24-30, Dec. 1999.
[7] M. Raya and J-P. Hubaux, "Securing Vehicular Ad Hoc Networks,"J. Computer Security, special issue on security of ad hoc and sensor networks, vol. 15, no. 1, pp. 39-68, 2007.
[8] N.B. Salem and J-P. Hubaux, "Securing WirelessMesh Networks," IEEE Wireless Comm., vol. 13, no. 2, pp. 50-55, Apr. 2006.
[9] 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.
[10] I.F. Akyildiz, X. Wang, and W. Wang, "Wireless Mesh Networks: A Survey," Computer Networks, vol. 47, no. 4, pp. 445-487, Mar.2005.

S.Parvaiz *was* born in proddatur, A.P, India. He received the B. Tech (IT) degree from the Madina Engineering College, kadapa in 2010: and Pursuing M.Tech (Computer Science) from the Audisankara college of engineering and technology, Gudur.