International Journal of Research

International Journal of Research (IJR)

e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 11, November 2015

Available at http://internationaljournalofresearch.org

Providing Security in Wireless Mesh networks

Maddula Bhupal Reddy[1]& P Dayakar[2]

[1]M-Tech Dept.Of CSE MLR Institute Of Technology TS, Hyderabad.

Mail Id: - BHUPAL777@GMAIL.COM

[2]Asst Professor Dept.Of CSE MLR Institute Of Technology TS, Hyderabad.

Mail Id: - Poreddydayakar2@Gmail.Com

ABSTRACT: -

A wireless mesh is a communication network composed of radio nodes organized in a mesh topology. A wireless mesh network avail users to stay online anywhere, anytime for an illimitable time and it provide high security.In this paper we come across two issues one is anonymity and other is traceability. Anonymity provides aegis for users to relish network accommodations without being traced. Now a day's Anonymity has received incrementing attention in the literature due to the users' vigilance of their privacy. Anonymity-cognate issues have been extensively studied in payment-predicated systems such as e-cash and peer-to-peer (P2P) systems, little effort has been devoted to wireless mesh networks (WMNs). The network ascendancy requires conditional anonymity such that misconducting entities in the network remain traceable.so in order to provide high network security we provide a secure architecture to ascertain unconditional anonymity for veracious users and traceability of misconducting users for network ascendant entities in WMNs. This architecture strives to resolve the conflicts between the anonymity and traceability objectives.Finally the architecture assuring fundamental security requisites such as authentication, confidentiality, data integrity, and no repudiation.

Keywords—Anonymity; traceability; pseudonym; misbehavior; revocation; wireless mesh network (WMN)

1. INTRODUCTION

Traceability is the ability to map events in cyberspace, particularly on the Internet, back to authentic-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 perpetuated as the technology has transmuted. The underlying reason for this perpetuating failure is a lack of economic incentives for amelioration. The lack of traceability at the edges is further illustrated by an incipient method of purloining another person's identity on an Ethernet Local Area Network that subsisting implements and procedures would entirely fail to detect. Anonymity and privacy issues have gained considerable research efforts, which have fixated on investigating anonymity in different context or application scenarios. One requisite for anonymity is to unlink a user's identity to his or her categorical activities, such as the anonymity consummated 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 additionally required to obnubilate the location information of a utilizer to avert kineticism tracing, as is paramount in mobile networks and VANETs. In wireless

communication systems, it is more facile for an ecumenical 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 incognito path between them. Nevertheless, unconditional anonymity may incur insider attacks since misconducting
Users are no longer traceable. Therefore, traceability is highly desirable such as in e-cash systems, where it is utilized for detecting and tracing double-spenders. A wireless mesh network (WMN) is a communications network composed 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 contrivances 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 sundry wireless technology including 802.11, 802.15, 802.16, cellular technologies or amalgamations of more than one type.

Wireless mesh network can be visually perceived as a special type of wireless ad-hoc network. Wireless Mesh Networks (WMNs) have become the focus of much research since they sanction for incremented coverage while retaining the captivating features of low cost and facile deployment. WMNs have been identified as key technology to enhance and compliment subsisting network installations as well as provide access where traditional technology is not available or too costly in install. A WMN is composed of mesh routers (MRs), which have inhibited or no mobility, and mesh clients (MCs) which are often plenarily mobile. The mesh routers form the backbone of the network sanctioning the clients to have access to the network through the backbone. We propose an algorithm for fair scheduling in WMNs with multiple gateways. We withal propose another algorithm for scheduling which places more accentuation on throughput while retaining a rudimentary level of throughput called commixed-partialness. 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 plenarily mobile.

Therefore, utilizing protocols designed solely for either of these networks alone does not capitalize on some of the most salutary features of WMNs. In MANETs all nodes are routers and suffer from inhibited power and bandwidth. In a WMN the MRs have more preponderant resources available than the MCs which is a property that may be exploited. Albeit a plethora of research efforts have been made to address these quandaries and some incipient specialized algorithms have been proposed categorically for WMNs, there are still many challenges in the area. Many of the subsisting solutions make many posits that can be relaxed to sanction 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 plenarily 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 virtually 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 utilizer identities from activities, as well as the traceability of misconducting users. Furthermore, the proposed pseudonym technique renders utilizer location information unexposed. Our work differs from antecedent 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 pristine anonymity scheme for payment systems among bank, customer, and store cannot be directly applied. In integration to the anonymity scheme, other security issues such as authentication, key establishment, and revocation are critical in WMNs to ascertain the correct application of the anonymity scheme. Moreover, albeit we employ the widely used pseudonym approach to ascertain network access anonymity and location privacy, our pseudonym generation does not rely on a central ascendancy.

2. RELATED WORK

Existing system:

In wireless communication systems, it is more facile for an ecumenical 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 incognito path between them. Nevertheless, unconditional anonymity may incur insider attacks since misconducting users are no longer traceable. Therefore, traceability is highly desirable such as in e-cash systems where it is utilized for detecting and tracing double-spenders.

Disadvantages:

No traceability

No pseudonym approach

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 plenarily 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 virtually 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 utilizer identities from activities, as well as the traceability of misconducting users. Furthermore, the proposed pseudonym technique renders utilizer location information unexposed.

Advantages:

Our work differs from anterior 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 pristine anonymity scheme for payment systems among bank, customer, and store cannot be directly applied. In additament to the anonymity scheme, other security issues such as authentication, key establishment, and revocation are critical in WMNs to ascertain the correct application of the anonymity scheme. Moreover, albeit we employ the widely used pseudonym approach to ascertain network access anonymity and location privacy, our pseudonym generation does not rely on a central ascendancy, e.g., the broker , the domain ascendancy , the conveyance ascendancy or the manufacturer, and the trusted ascendancy , who can derive the user's identity from his pseudonyms and illicitly trace a veracious utilizer. Our system is not intended for achieving routing anonymity, which can be incorporated as an enhancement.

3. IMPLEMENTATION

Wireless mesh networks (WMNs)

The wireless mesh backbone consists of mesh routers (MRs) and gateways (GWs) interconnected by mundane wireless links (shown as dotted curves). Mesh routers and gateways accommodate 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 accommodates as a trusted ascendancy the central server of a campus WMN.

Blind Signature

In general, a blind signature scheme sanctions 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 designation suggests, this property restricts the utilizer in the blind signature scheme to embed some account-cognate secret information into what is being signed by the bank (otherwise, the signing will be unsuccessful) such that this secret can be recuperated by the bank to identify a utilizer if and only if he double-spends. The restrictiveness property is essentially the assurance for traceability in the restrictive blind signature systems.

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 predicated on the misconduct history of the client, which reflects the server manager's confidence about the client to act congruously. Ticket issuance occurs when the client initially endeavors to access the network or when all antecedently issued tickets are depleted. The client needs to reveal his authentic ID to the server manager in order to obtain a ticket since the server manager has to ascertain the authenticity of this client.

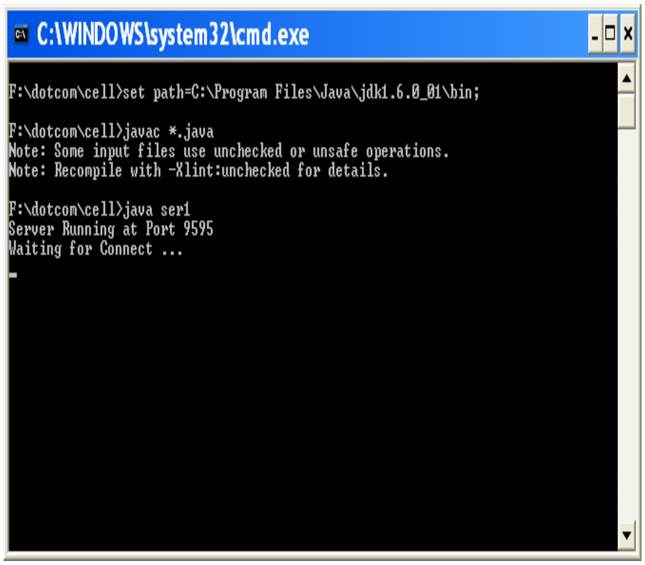
Fraud Detection

Fraud is utilized interchangeably with misconduct 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 misconduct, which causes the server manager to constrain his ticket requests.

Fundamental security objectives

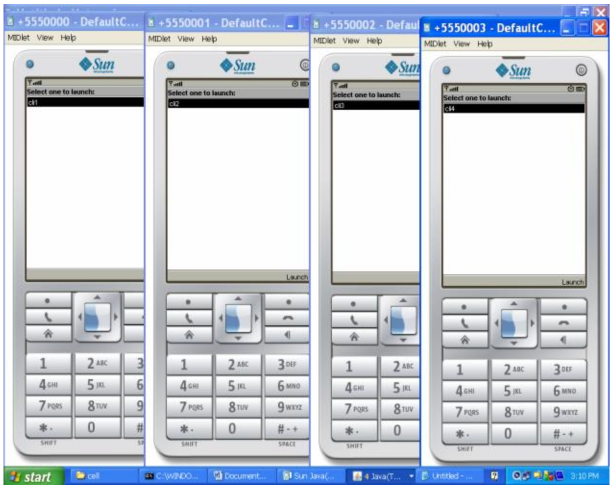
It is picayune to show that our security architecture slakes the security requisites for authentication, data integrity, and confidentiality, which follows directly from the employment of the standard cryptographic primitives, message authentication code, and encryption, in our system. We are only left with the proof of nonrepudiation in this category. A fraud can be repudiated only if the client can provide a different representation, he kens of message from what is derived by the server manager. If the client has misconducted, the representation he kens will be identically tantamount to the one derived by the server Manager which ascertains nonrepudiation. Ad hoc networks inherit some of the traditional quandaries of wireless communication and wireless networking

4. EXPERIMENTAL RESULT


C:\WINDOWS\system32\cmd.exe

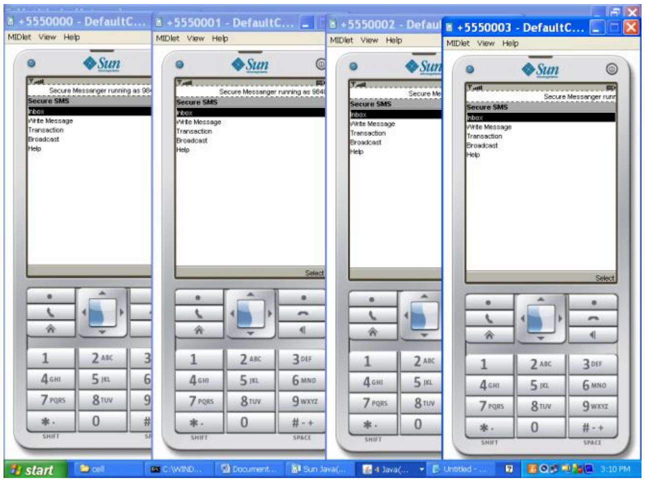
```
F:\dotcom\cell>set path=C:\Program Files\Java\jdk1.6.0_01\bin;

F:\dotcom\cell>javac *.java
Note: Some input files use unchecked or unsafe operations.
Note: Recompile with -Xlint:unchecked for details.

F:\dotcom\cell>java ser1
Server Running at Port 9595
Waiting for Connect ...
_
```

Fig:1Server Started and is waiting for clients


+5550000 - DefaultC... | +5550001 - DefaultC... | +5550002 - Defaul | +5550003 - DefaultC...

Select one to launch:
cl1 | cl2 | cl3 | cl4

Fig:2Clients have now started and are now waiting for approval


+5550000 - DefaultC... | +5550001 - DefaultC... | +5550002 - Defaul | +5550003 - DefaultC...

Secure Messanger running as 98...

Fig:3Clients are now connected to the server

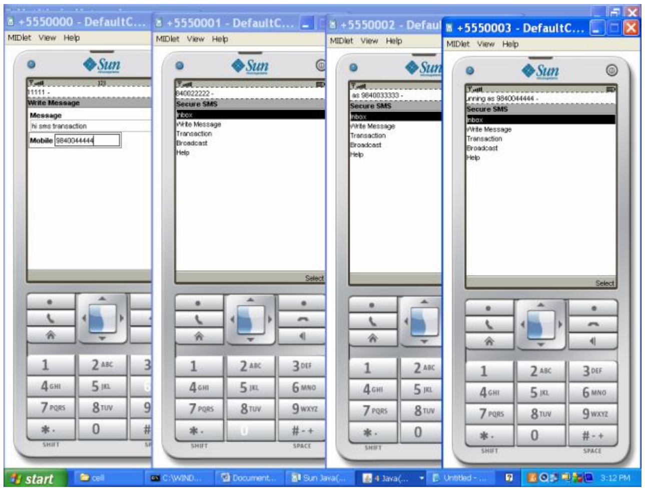
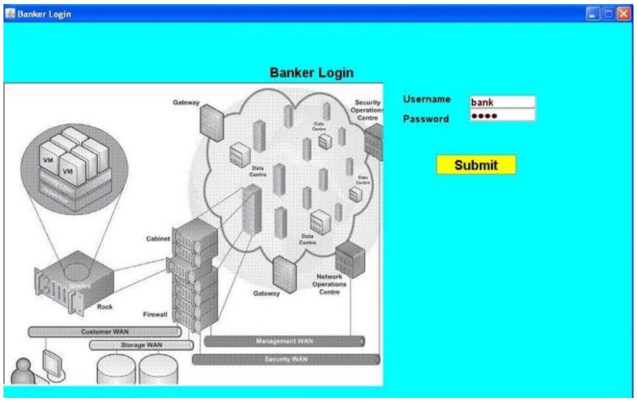

11111 -
Write Message
Message
hi sms transaction
Mobile 9840044444

Fig: 4 Client 1 sending a message to client 4

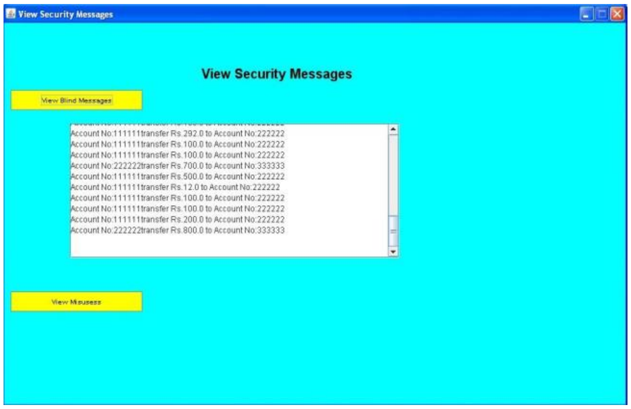

Banker Login

Banker Login

Username bank
Password ••••

Submit

Fig: 5 Bankers Logging in



```
Account No:111111transfer Rs.292.0 to Account No:222222
Account No:111111transfer Rs.100.0 to Account No:222222
Account No:111111transfer Rs.100.0 to Account No:222222
Account No:222222transfer Rs.700.0 to Account No:333333
Account No:111111transfer Rs.500.0 to Account No:222222
Account No:111111transfer Rs.12.0 to Account No:222222
Account No:111111transfer Rs.100.0 to Account No:222222
Account No:111111transfer Rs.100.0 to Account No:222222
Account No:111111transfer Rs.200.0 to Account No:222222
Account No:222222transfer Rs.800.0 to Account No:333333
```

Fig: 6 Banker checking the various transactions performed

5. CONCLUSION

We propose SAT, a security architecture mainly consisting of the ticket-predicated protocols, which resolves the conflicting security requisites of unconditional anonymity for veracious users and traceability of misconducting users. By utilizing the tickets, self-engendered pseudonyms, and the hierarchical identity-predicated 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 quandary prevalent in P2P communication systems is the free-riding, where some peers capitalize on the system by providing little or no accommodation to other peers or by leaving the system immediately after the accommodation needs are satiated. Peer cooperation is thus the fundamental requisite for P2P systems to operate opportunely. Since peers are postulated 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-predicated approaches. In the reputation-predicated systems, peers are penalized or rewarded predicated on the observed demeanor. However, low availability remains an unobservable deportment in such systems, which obstructs the feasibility of the reputation-predicated mechanism in ameliorating peer availability. By contrast, the payment-predicated 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.