ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 3, pp: (46-52), Month: July - September 2014, Available at: www.researchpublish.com

Finding Forgery Attacks in WMN by Secure and Dependable Ticket Based Tracing System

Anil Kumar.T[1], Bharathi.M.A[2]

PG Student[1], Associate professor[2]
Department of Computer Science and Engineering
Reva Institute of Technology and Management, Bangalore, India

Abstract: **A very important component in any network deployment now a day's is Privacy. Users are willing to enjoy the network services without letting their identity. Anonymity comes in to picture which means not letting the user identity whenever he is accessing the benefits of the network. This anonymity condition is important for few services e.g. Social Networking. But there are few services where user has to revel his identity e.g. on-line payment system, Internet banking or on-line transaction. Wireless Mesh Network (WMN) are our main targets. However, not all the users are honest when they are using the network services; there are certain situations where users are involved in misbehaving activities. To revels user identity Consequently we need a system. Pseudonym techniques are suitable for this kind of problems. The honest users and misbehaving users in the Wireless mesh network are conditionally traced out by this system. In this paper, A Secure Ticket Based tracing system is developed that mainly serves the above specified condition. Furthermore this proposed architecture not only used to trace the user activities, it is also guaranties to hold the fundamental security aspects like validation, endorsement, Data Protection.**

Keywords: **Pseudonym; Anonymity; misbehavior; Wireless Mesh Network; Tickets.**

I. INTRODUCTION

Wireless Mesh Network is a promising technology to meet the challenges of the present generation for providing flexible adaptive and reconfigurable architecture. Wireless Mesh Network provides cost-effective business solutions. The network topology of a typical of a typical WMN depicted in the above figure. The wireless mesh backbone consists of mesh routers (MR), gateway (GW), they are connected normal wireless links. The access points here are GW, MR. They are finally connected to Internet. This topology mainly can be seen in Hospital, Campus, Enterprise and residential buildings.

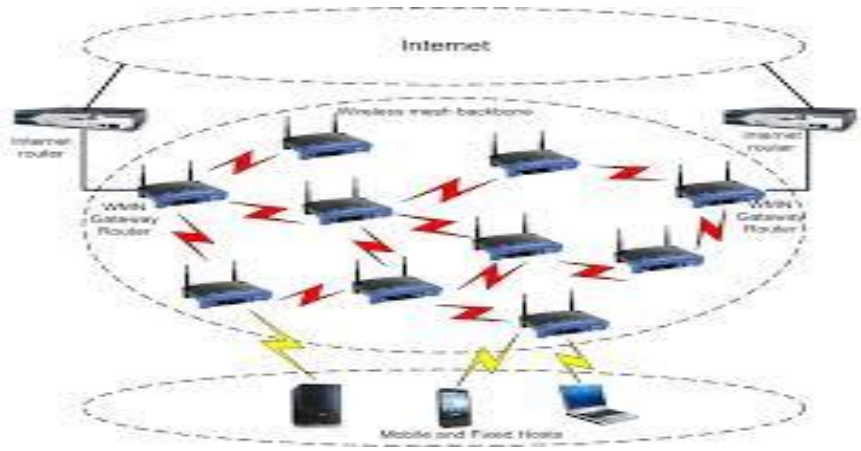

Fig 1. Network topology of a typical WMN

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 3, pp: (46-52), Month: July - September 2014, Available at: www.researchpublish.com

The cloud represents the service providers, where each service providers will have a Trusted Authority (TA) or Trusted Manager(TM). The solid and bold dash lines represent the association of TA and gateways with wired and wireless links respectively. Intensive task are handled by this gateway's and TM.

Security is the important factor that has to be considered before deploying any network. Wireless security is the hot topic in the literature for various network technologies. Anonymity and privacy issue have considerably gained a lot of attention [2][3]. Anonymity is important to hide the location information of the user to prevent tracing. Users are provided with the anonymity privileges to enjoy the services in the network [7]. There are certain situations where user might involve in doing some internal attacks, which here we are considering as the Forgery attacks. Once the user gains the access to the network it's not guarantee that all users will be loyal to the services which they are accessing. Misbehaving activities will takes place inside the network. In this Ticket based tracing system every user is provided with the Tickets, which are nothing but some of the access permissions inside the network. Even though tickets are provided users try to access non ticket services. Traceability becomes important to conditionally differentiate between the honest users and misbehaving users. In this paper we are motivated to remove the misbehaving users when internal attacks are made in our wireless mesh network. The initial system design was [1] which gives the idea of Ticket based secure system. But in this [1] we were not able to clearly understand the quality and usage of the architecture fully. As a result we provide a clear and detailed performance and feasibility in this paper. Wireless Spoofing attack will significantly impact the performance of network. To prevent this IP Spoofing attack we are implementing our tracing system with the filter [4].

Specifically the main scope of this paper includes 1) Providing Access to user via Issuing Tickets. 2) Forgery attack in depositing the ticket. 3) Sinkhole and IP spoofing attack to gain the unauthorized service or data. 4) List the fraud users in the network and remove these misbehaving users from the network by revoking the tickets which are issued.

II. RELATED WORK

In the system, as mentioned above Tickets are issued by the Trust Manager (TM). These tickets have to be deposited in the network before client gains the access. Here these tickets are nothing but the privileges given to users.

A. Ticket Issuance

To maintain the security of the network from the attack and to have the fairness between clients, the TM will have the access of each client by issuing tickets. Tickets from the TM will be issued depending of the client's misbehavior history. Ticket issuance takes place when client initially wants access to network or after tickets are revoked. The TM will not link the user identity with the ticket, because of this user will employ in blind identity to TM.

Some of the notations used here are as follows ->: single-hop communications;

->->: multi-hop communications; ||: concatenation;
IDx: Identity of an entity x;

PSx: the self-generated pseudonym by a client x by using his identity IDx; H1(IDx)/Γx: public/private key of the entity x;

PSx/Γx: the self-generated pseudonym/private key pairs based on the above public/private key pairs; SIGΓx (m): signature on a message m using Γx;
VER(SIG): verification process; symmetric encryption on plaintext D using the shared secret key k;
HMACk(m): keyed-hash message authentication code on amessage m using k;
C, TM, G : Client and Trust Manager, Gateway respectively;

1. C->->TM: IDC, m, t1, HMACK(m || t1);
2. TM->->C: IDTM, X=e(m,ΓTM), Y=e(P,Q), Z=e(m,Q),U=rH1(IDTM), V=rp,t2,HMACK(X|| Y || Z || U || V || t2);
3. C->->TM: IDC

B=1\λH2(m'||U'||V'||R||W||X'||Y'||Z')+μ, t 3,HMACK(B||t3);

4. TM->->C: IDTM, σ1=Q+BΓTA,σ2=(r+B) ΓTA +rH1(c),t4,HMACK(σ1||σ2||t4). B. Ticket Deposit

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 3, pp: (46-52), Month: July - September 2014, Available at: www.researchpublish.com

When client obtain a valid ticket, the client has to deposit it in the network to experience the network services[1]. This scheme restricts in depositing the ticket only once at the entry. Here a batch of tickets is issued each time and the client may hold unused tickets. Since there won't be any separate expiry time for the tickets issued, they will expiry at once.

1. C->->G:PSC,m',W,c, σ = (U',V',X', ρ,σ' 1,σ' 2),t5, SIGΓc~(m'|| W || c||σ||t5);
2. G->->C:IDG,d=H3(R||W||IDG||T), t6,HMACK(d||t6);
3. C->->G:PSC,r1=d(u1α)+v1, r2=dα+v2,t7,HMACK' (r1||r2||t7); and
4. G->->C:IDG,misb,exp,t8,SIGΓG(PSC|| IDG||misb || exp || t8) . C. Ticket Revocation

When the client is compromised, reveling all his identity and secret to the advisory the tickets will be revoked. A valid revocation must be sent by compromised user to gain genuine tickets again. A record of the revocation report will be sent to the TA, which will update and distributes the tickets to the users again.

The main retreat is, Tickets which are deposited by one user might deposit by even others, i.e. if User A is provided with ticket number 2, and User B is provided with ticket number 3 then if A indulges in having the access of B, by knowing B's ticket number, A can clearly go ahead and deposit the Ticket[6]. Attacks showed that the client can impersonate the Pseudonym Manager to sign some tickets. There was no sign of tracing the misbehaving users. Clients who deposit the wrong ticket only traced. Cryptographic techniques which are used to provide the security for the data was not up to the expectation, i.e. DES techniques were used. Analysis clearly showed that Ticket Based anonymity scheme cannot satisfy the traceability [6].

III. PROPOSED SYSTEM

Pseudonym manager will first have the access to the network. He will set a system .The next step of PM is to create a new user who seeks to enter in to the network. PM will be granting the tickets along with the user creation. Now user has to get connected to the servers to enter in to the Wireless Mesh Network through the Server. Server will be collecting all the activities of the user. If the user under goes any misbehaving activates which we have mentioned in above section, the report of that will be provided to the PM. User will have the credential Acquisition to the WMN. The below section let us see how the user will misbehave and how it has been controlled.

A. Forgery Attack In Depositing The Ticket

Forgery, Fraud and misbehaving are used interchangeably in this section, which is mainly an insider attack. The reuse of ticket from the user generally means that whenever user fails to acquire the tickets from the PM. This may be due to the past misbehaving history of the user which causes the PM to constrain the ticket request. Multiple-Deposit can also be termed users coalition, which is useful when the coalescing parties are unauthorized users with misbehaviour history having difficulty in acquiring ticket from the PM.

A possible remedy to this situation is to specifying the no overlapping activity period of a ticket instead of merely the expiry date/time such that each time only 1 ticket is deposited. Another solution is to adopt the tamper proof secure module so that a client or user cannot disclose his secret to other parties. This approach will eliminate the multiple deposits of tickets. PM Will detect duplicate deposit using the ticket record report by the Server.

Fig 2: Valid ticket deposition by user

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 3, pp: (46-52), Month: July - September 2014, Available at: www.researchpublish.com

Fig 3: Invalid ticket deposition by user, misbehaving details sent to PM.

Here we are linking the user Identity with the tickets, which will be issued to the user. If the client or the user misbehaves, the client anonymity is no longer guaranteed because PM will identify this user, and accordingly penalize him by revoking the client network access privileges by investing traceability property offered by our security architecture.

B. Sinkhole Attack

The sinkhole attack is a particular node attack that prevents the base station from obtaining complete and correct data, thus forming a serious threat to higher level protocols[8]. In a sinkhole attack, a compromised node tries to draw all or as much traffic as possible from particular nodes. Making it look attractive to the surrounding nodes with respect to the routing metric values .Figure 1 explains how malicious node redirects with modified route sequence numbers. Here malicious node sends greater sequence number to misguide that it is a fresh route. Figure 2 depicts how malicious node redirects with modified hop count. Here malicious node sends lesser hop count value to tell that this is shortest path. In fact there is no such path exists. Node A assumes that the route through M is the shortest route and sends any packet to the destination through it. When the node A sends data to M, M absorbs all the data. So the attacks can be accomplished [9].

C. IP Spoofing

In networking the term IP address Spoofing or IP spoofing refers to the creation of internal protocols packets with forged origin [5]. IP address, call spoofing, with the purpose of concealing the identity of sender or impersonating another computing system. The basic protocol sending data over the Internet network and many other computer network is IP. The packet with IP header contains, along with other things, the numerical sender and receiver address of the packet.

IV. SYSYEM DESIGN AND ARCHITECTURE

The proposed software solution, illustrated in Figure, comprises the following four parts: pseudonym Manager, user, server and WMN.

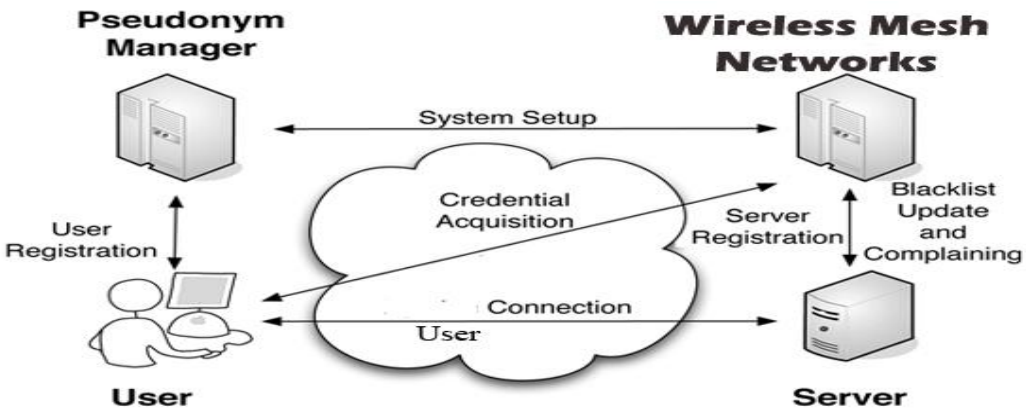

Fig.4: System Architecture.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 3, pp: (46-52), Month: July - September 2014, Available at: www.researchpublish.com

System architecture which is shown in Fig 4 considered being the conceptual design that defines the structure and behavior of a system. Large systems are always decomposed into sub-systems that provide some related set of services. The initial design process of identifying these sub-systems and establishing a framework for sub-system control and communication is called Architecture design and the output of this design process is a description of the software architecture. An architecture description is a formal description of a system, organized in a way that supports reasoning about the structural components and their relationship in order to work as a system. It defines the system components or building blocks and provides a plan from which products can be procured, and systems developed, that will work together to implement the overall system.

The overall logical structure of the project is divided into processing modules and conceptual data structures are defined as Architectural Design as shown in fig 5

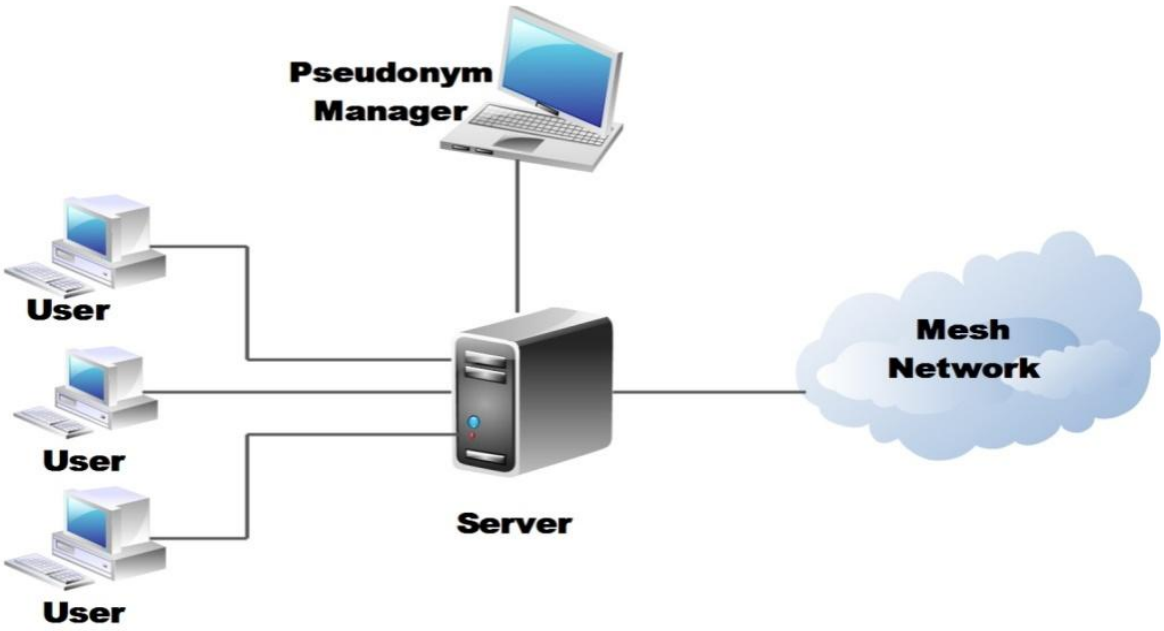

Fig 5: Project Setup for Ticket Based Tracing System

The architectural design process in Fig 5 is concerned with establishing a basic structural framework for a system. It involves identifying the major components of the system and communications between these components.

Pseudonym manager will first have the access to the network. He will set a system .The next step of PM is to create a new user who seeks to enter in to the network. PM will be granting the tickets along with the user creation. Now user has to get connected to the servers to enter in to the Wireless Mesh Network through the Server which is shown in architecture. Server will be collecting all the activates of the user. If the user under goes any misbehaving activates the report of that will be provided to the PM. User will have the credential Acquisition to the WMN.

V. IMPLEMENTATION

The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

Main Modules

- Pseudonym Server
- Pseudonym Manager
- Remote User
- Tickets/ Access Privilege

VI. RESULTS AND ANALYSIS

Our Security architecture will clearly shows about the internal attack that user may indulge. Depending on these attacks, the system has proposed a solution for attacks i.e. Forgery attacks in depositing the tickets, Sinkhole attack which is considered as a serious threat in the network, IP Spoofing which the system will control the attack by implementing the ingress filter technique. This is considered to be the secure in ticket based tracing system for conditional anonymous user and tracing misbehaving users in anonymous Wireless Mesh Network. Below Fig(6) show the Tickets or privileges provided to the users and number of attempts where he misbehave. X-axis shows the type of tickets issued and Y-axis show the number attempts. This system helps us to understand where exactly the number attack happens.

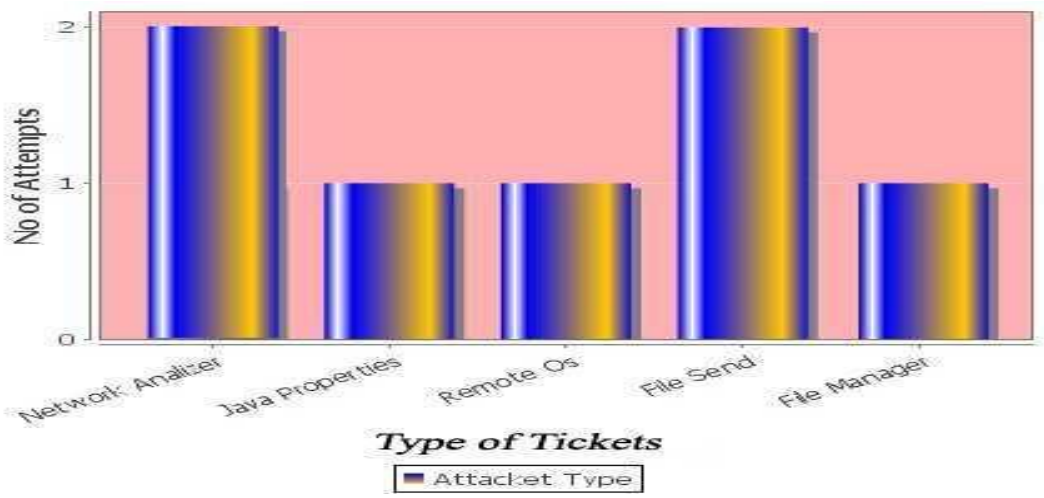

Fig 6: Type of tickets issued and number of misbehaving attempts made.

VII. CONCLUSION

The principles behind next generation network security architectures proposed by various parties to address some of the most critical shortcomings faced by the Internet today. The proposed solutions while successful in solving the issues of resolve the conflicts between the unconditional anonymity for honest users and traceability of the misbehaving users. Internal attacks are clearly seen and have the perfect solution to prevent. Misbehaving users will no longer exist in the network to use any further services, they are completely eliminated. The proposed architecture is demonstrated to achieve desired security objective and efficiency. The future work of this may include the implementation of different types of filters for IP Spoofing.

REFERENCES

[1]. J. Sun, C. Zhang, Y. Zhang, and Y. Fang, " SAT: A Security Architecture Achieving Anonymity and Traceability in Wireless Mesh Networks," IEEE Trans. Dependable and Secure Computing, vo l. 8, no. 2, pp. 295-307, 2011.

[2]. 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.

[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]. Jie Yang, Yingying (Jennifer) Chen, Wade Trappe, and Jerry Cheng " Detecting, Determining and Localizing Multiple Spoofing Attackers in Wireless Networks". Ieee transactions on parallel and distributed systems, vol. 24, no. 1, january 2013

[5]. Ezra Kissel, University of Delaware and Jelenairkovic, USC/ISI" Comparative Evaluation of Spoofing Defenses"

[6]. Huaqun Wang and Yuqing Zhang, Member, IEEE" On the Security of a Ticket Based Anonymity System with Traceability Property in Wireless Mesh Networks" IEEE transactions on dependable and secure comput ing, vol. 9, no. 3, may/june 2012.

[7]. Matt Blaze1, John Ioannidis2, Angelos D. Keromytis3, Tal Malkin3, and Avi Rubin" Anonymity in Wireless Broadcast Networks" International Journal of Network Security, Vol.8, No.1, PP.37–51, Jan. 2009.

[8]. HassenRedwan and Ki-Hyung Kim Department of international communication and Engineering" Survey of Security Requirements, Attacks and Network Integration in Wireless Mesh Networks" Japan-China Joint Workshop on Frontier of Computer Science and Technology 2008.