IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 16, Issue 4, Ver. VII (Jul – Aug. 2014), PP 01-05
www.iosrjournals.org

Pseudonym Based Security Architecture for Wireless Mesh Network

Ms. Sharvani R. Marathe[1], Dr. Santosh L. Deshpande[2]
[1](Department of Computer Network Engineering, Visvesvaraya Technological University, Belgaum, India)
[2](Department of Computer Network Engineering, Visvesvaraya Technological University, Belgaum, India)

Abstract : *Wireless Mesh Network (WMN) is a wireless network with mesh topology and is expected to be widespread due to the advantages such as low deployment cost, easy maintenance, robustness, scalability, reliable service coverage and high performance. It has self-configuring and self-healing ability and is compatible, interoperable with existing wireless networks. With these advantages, WMN inherits security issues that need to be considered before the deployment and proliferation of the network, as it is unappealing to subscribers to obtain services without security and privacy. It is difficult to achieve both, privacy and security together in a system but an attempt is made by designing a ticket-based security architecture achieving anonymity and traceability in WMN. Anonymity provides protection to the users to access network services without being traced i.e. preserving the identity of the user and has been extensively studied in payment-based systems such as e-cash and peer-to-peer systems. When anonymity is achieved, few entities tend to misbehave by imposing attacks as they remain anonymous. This affects network security and hence, misbehaving entities have to be traced. The clustering concept is included in the system to increase network performance and to reduce topology updating overhead in the network.*

Keyword: *Anonymity, traceability, pseudonym, misbehavior, clustering.*

I. Introduction

Wireless Mesh Network (WMN) is a promising technology. It is expected to be widespread due to low deployment cost, easy network maintenance, robustness, scalability, reliable service coverage and high performance. WMN has self-configuring ability and self-healing ability [1].

WMN has many security issues such as eavesdropping, denial of service, replay attack [2]. These issues need to be considered before deployment and proliferation of the network. Anonymity is one of the security issues in WMN which has received attention as the users are concerned about privacy. Anonymity provides protection for the users to access network without being traced. It is also required to hide the location information of a user to prevent the movement tracing, as it is easier for a global observer to mount traffic analysis in wireless communication systems. Anonymity provides privacy, but it may incur insider attacks as the misbehaving users are no longer traceable. To avoid such attacks, traceability of misbehaving users must be ensured.

The proposed system is a ticket based security architecture. This architecture resolves the above issues by achieving anonymity for honest users and traceability of misbehaving users based on the article [3]. In the proposed system, tickets are issued to the users. Tickets are time limited cryptographic messages providing access to network services. To achieve anonymity, the issued tickets must not be linkable to the user's identity. The restrictive partially blind signature technique is used to make ticket discrete from user's identity. The restrictive partially blind signature technique [4] allows a recipient to obtain signature on a message without revealing anything about the message to the signer, but the choice of message to be signed is restricted and must conform to certain rules. This restriction helps in traceability. In addition, the technique allows the signature to convey publicly visible information such as expiration date, collateral conditions etc. on common agreements between signer and signee. This publicly available information is useful when certain information in the signature needs to be reviewed by a third party for verification. Location privacy is achieved by using pseudonym technique [5]. In this technique, the real ID of a user is substituted with a pseudonym which can be a name or a number. The proposed system uses identity based cryptography (IBC) [6], [7] for authentication. In IBC, the public key of a user is derived from his public identity information such as email address. It consumes less time when compared to the use of digital certificates for authentication.

Clustering is a process of organizing mobile nodes into groups called clusters. The nodes within a particular range are grouped to form a cluster. Each cluster has only one cluster head which has the complete knowledge about group membership and link state information within a cluster. Clustering helps in obtaining scalability, achieving high performance and balancing load in large wireless networks with mobile nodes [8]. To attain these advantages, the proposed work introduces clustering in WMN. This cluster based system minimizes the updating overhead during topology change due to mobility of mesh nodes.

II. Security architecture

To maintain network security against attacks and fairness among clients, a security architecture is proposed in the present work. This security architecture is based on issuing tickets and consists of ticket issuance, ticket deposit and fraud detection protocols. The security architecture uses identity based cryptography; restrictive partially blind technique and pseudonym concept to achieve anonymity for honest clients and traceability for dishonest clients. In addition to security measures, the proposed system includes clustering mechanism to achieve scalability and high network performance in WMN.

1) Ticket Issuance

The first step is registration of a client at trusted authority (TA). In registration, the client's authentication is verified. The proposed system uses identity based cryptography for authentication. To prove authenticity, the client first sends his real ID for registration which can be an email address. The TA verifies email address by sending nonce to it. The successful return of nonce to TA confirms authenticity of the client. After authentication, the TA creates an account for client, stores client's real ID and misbehavior value in it. This misbehavior is initially set to zero as the client is initially considered to be honest. The account number is sent back to client, which the client uses for requesting a ticket.

After successful registration, the client sends ticket request to TA which includes the account number. The TA then checks the account and generates a ticket using restrictive partially blind signature technique. The ticket includes parameters such as, ticket serial number, expiry time, traffic access, misbehavior field and TA's signature. The TA's signature is a restrictive blind signature on account number which is helpful during traceability of dishonest client. The ticket serial number, expiry time, traffic access and misbehavior parameters are the resultant of partially blind signature. These parameters are used for verification. Thus the ticket generated is restrictive partially blind signature. This ticket does not reveal client's identity. The ticket generated is issued to the client.

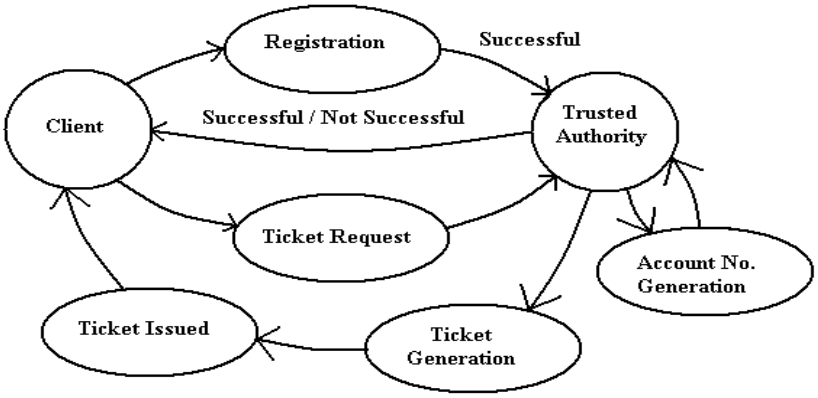

Figure 1: State Diagram of Registration and Ticket Issuance.

2) Ticket Deposit

The issued ticket can be used any time later before ticket expiry, but it can be deposited only once at the first encountered gateway. When the client wishes to access the network, he deposits the issued ticket and a pseudonym at the gateway. This pseudonym is an alternative name or a number, used by the client as a substitution for his real ID for achieving anonymity and location privacy. The pseudonym is generated by the client and it cannot be changed while using the corresponding ticket. Changing pseudonym frequently helps in achieving high degree anonymity and thus, the client can use different pseudonyms while accessing different tickets.

At the gateway, when a {ticket, pseudonym} pair is deposited, the ticket is verified with the help of TA's signature. Then the gateway generates a corresponding ticket record. This ticket record consists of ticket serial number, expiry time, traffic access, TA's signature and misbehaving value. After verification of the ticket, if no misbehavior is detected, network access is granted to the honest client based on the traffic access and expiry time parameters of the ticket. For honest client, the ticket record generated is sent to the TA periodically. During verification of the ticket, if misbehavior is detected, the ticket record generated is sent to TA before granting access. The gateway then waits for TA's feedback. If the TA sends a positive feedback, then the gateway grants network access to the client. If the feedback is negative, the client's access to the network is denied.

3) Fraud Detection

Fraud is used interchangeable with misbehavior. Ticket reuse and multiple deposits are the two types of fraud considered. The ticket reuse generally results when the client is unable to obtain ticket for desired network access due to his misbehavior. Multiple deposit results when the unauthorized users or clients with misbehavior history have difficulty in obtaining tickets. In multiple deposit, the client distributes the {ticket, pseudonym} pair to unauthorized users, so that they can access network simultaneously by depositing the pair at another gateway. These two types of fraud are addressed in the proposed security architecture. Both the frauds are detected by the TA with the help of ticket record reported by the gateway. Whenever such fraud is detected or the misbehavior value in the ticket record is non-zero, the TA traces the misbehaving client with the help of TA's signature in the ticket record. The TA's signature includes account number and when this account number is obtained, the real ID of misbehaving client is traced. This misbehavior of the client is added to the past misbehaving history in the account which will be referred during ticket generation. If the resulting misbehavior value is within a pre-defined threshold, a positive feedback is sent to the gateway, signifying that the client is allowed to access network. If the misbehavior value crosses the threshold, a negative feedback is sent to the gateway. This negative feedback signifies that the client cannot access network.

The techniques presented above, resolves the conflict between anonymity and traceability. As long as the client is a well-behaved user in the network, his anonymity can be fully guaranteed. This is achieved by blinding process of the ticket issuance protocol, where the TA knows the client's real ID but does not know which {ticket, pseudonym} pair belongs to that client, while the gateway knows the linkage between ticket and pseudonym but learns no information on the real identity of the owner of the pair. Thus the linkage between the ticket and the identity is broken and anonymity is achieved. On the other hand, if the client misbehaves, the TA tends to identify the client. This ensures traceability of the misbehaving client and his anonymity is no longer guaranteed.

In the proposed system, all the data communicated over WMN is encrypted using RSA algorithm. The key required for encryption is exchanged between communicating parties using Diffie-Hellman algorithm. The anonymity of client and encryption of data address the eavesdropping security issue. The ticket serial number, expiry time and the condition that the ticket can be deposited only once, prevents replay attack. The TA's control over issuance of tickets to a client, addresses denial-of-service. The pseudonym of client is hashed which can be used for client verification in case of mobility of client from one gateway to another. This addresses the issue of multiple deposit of same ticket at different gateways by client.

4) Clustering concept

Clustering is a process of organizing nodes into groups called clusters. The proposed system which is a cluster-based architecture consists of clusters. Each cluster has a cluster head which monitors the nodes within the cluster. The proposed system considers access routers as cluster head and the nodes within its range as cluster members. The communication data of a cluster member should pass through the respective cluster head. The cluster-based WMN minimizes the topology updating overhead due to mobility of nodes.

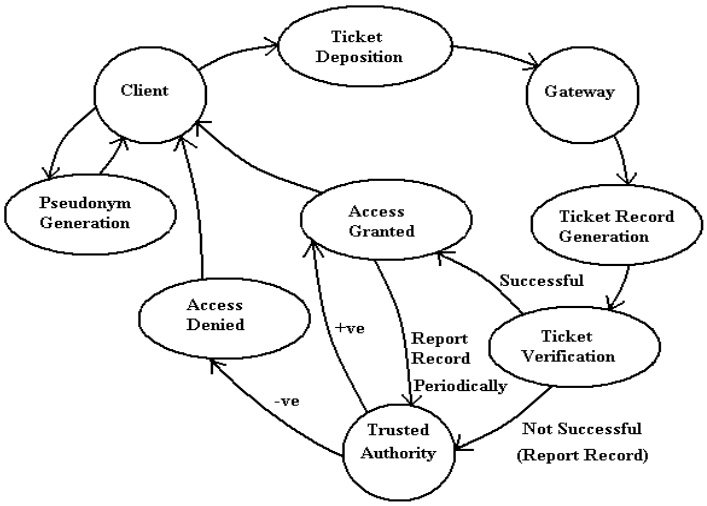

Figure 2: State Diagram of Ticket Deposit and Fraud Detection.

III. Result analysis

MATLAB is used for simulation of the system.

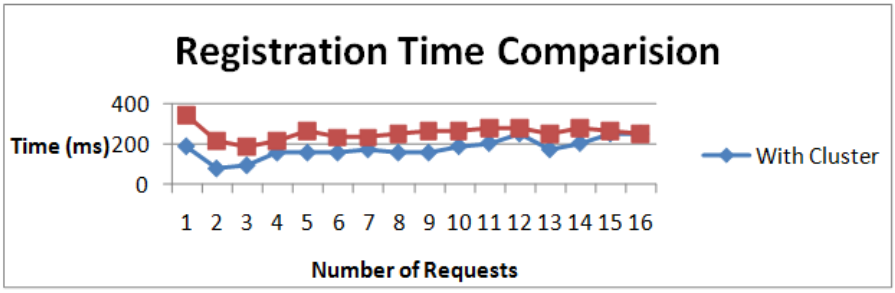

Figure 3: Graph of Registration Time Comparison.

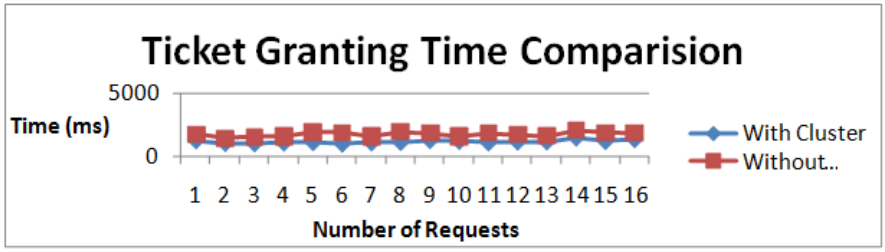

Figure 4: Graph of Ticket Granting Time Comparison.

The graphs represent the comparison for registration time and ticket granting time between a system with clustering and a system without clustering. This shows that the system with clustering takes less time for registration when compared with the system without clustering.

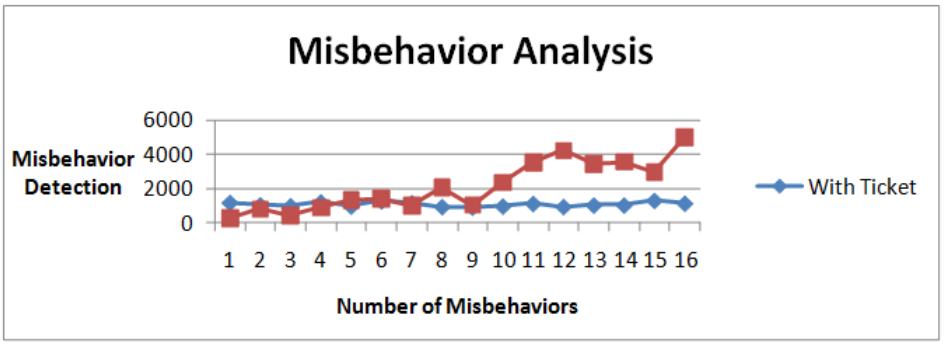

Figure 5: Graph of Misbehavior Analysis.

The graph represents the time comparison for misbehavior analysis between a ticket-based system and a system without ticket. In the ticket based system, the ticket is verified by gateway during ticket deposition and the corresponding ticket-record is reviewed periodically by TA when the client is accessing network service. This helps to detect misbehavior of client early when compared to a system without ticket.

IV. Conclusion

The proposed system achieves anonymity for honest users and traceability of the misbehaving users. The ticket-based architecture ensures controlled network access and addresses security issues such as, eavesdropping, denial-of-service and replay attack. With the help of graph it is shown that the ticket-based system is capable of early detection of misbehavior of user, when compared to a system without ticket. This early detection of misbehavior ensures controlled network access and maintains security of the network. The clustering concept reduces the topology updating overhead and achieves high performance in wireless mesh networks. The time consumption for communication in a clustered system reduces as shown in graph, thus increasing the performance of network.

References

[1] I. F. Akyildiz, X. Wang and W.Wang, Wireless Mesh Networks: A Survey, Computer Networks, vol. 47, no. 4, pp.445-487, Mar. 2005.
[2] 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.
[3] Jinyuan Sun, Chi Zhang, Yancho Zhang, Yuguang Fang, SAT: A Security Architecture Achieving Anonymity and Traceability in Wireless Mesh Network, IEEE Transaction on Dependable and Secure Computing, March-April 2011.
[4] X. Chen, F. Zang and S. Liu, ID-Based Restrictive Partially Blind Signatures and Applications, J. Systems and Software, vol. 80, no. 2, pp. 164-171, Feb. 2007.
[5] A. R. Beresford and F. Stajano, Location Privacy in Pervasive Computing, IEEE Pervasive Computing, vol. 2, no. 1, pp. 46-55, Jan.-Mar. 2003.
[6] Al-Sakib Khan Pathan, Security of Self-Organizing Networks MANET, WSN, WMN, VANET 2010.
[7] Yuguang Fang, Xiaoyan Zhu, Yanchao Zhang, Securing Resource-Constrained Wireless Ad Hoc Networks, IEEE Wireless Communications, April 2009.
[8] Jane Y. Yu and Peter H. J. Chong, A Survey of Clustering Schemes for Mobile Ad Hoc Networks, Nanyang Technological University.