A Ticket based Security Framework for Fast Transmission in Wireless Mesh Network

Priyanka Patel
Dept. of Computer Science
Acropolis Institute of
Technology & Research,
Indore, M.P., India

Abhay Kothari
Dept. of Computer Science
Acropolis Institute of
Technology & Research,
Indore, M.P.,India

ABSTRACT
In recent years, Wireless Mesh Network (WMN) has been emerged out as the next generation of wireless communication networks due to its economical feature in the era of broadband services it supports. However, security issues inherent in WMNs or any wireless networks needed to be considered before the deployment of such networks, since it is disagreeable to subscribers to acquire services without the assurance of security and privacy. Wireless security has become the hot are in the literature for diverse network technologies such as ad hoc networks, cellular networks, local area networks and sensor networks etc. On the other hand, the network authority necessitates the provisional anonymity such that all the misbehaving entities in the network remain traceable. This paper introduces a ticket based security framework to make sure the unconditional anonymity for honest users and traceability of misbehaving users. The proposed architecture strives to resolve the divergence between the anonymity and traceability, in addition to ensuring these objectives it also pledges the fundamental security requirements by providing the location privacy and without relying on the central authority.

General Terms
Wireless Mesh Network, Authentication, Security, etc

Keywords
Wireless Mesh Network (WMN), Security requirements, Authentication, Anonymity, Trusted Authority etc.

1. INTRODUCTION
Due to the dynamicity and self organizability of wireless mesh network (WMN), it has received the attention from the eminent researchers working in the dispersed research areas. It's widely spread heterogeneous applications has gain the popularity in health and medical systems and services to provide broadband services [1]. However, prior to the deployment and enabling of such networks, it has become mandatory for the subscribers to ensure the guarantee of privacy and security. Now a day the security concerns in the wireless network has become the primary concerns for diverse network technologies such as mobile ad hoc networks (MANETs) [2], [3], ad hoc networks (VANETs) [4], wireless local area networks (WLAN) [5] and wireless sensor networks [6], [7] etc. However, due to the advancements in the payment based systems, the authentication and traceability of anonymous users in the internet world has become a major concern. The feature of anonymity hides the user's geographical information in payment based systems. To avoid the misbehavior of network clients it has become necessary to not become dependable on central authority. Therefore to avoid the illegal tracing of authenticated users the traceability has become mandatory. To resolve such security conflicts, this paper proposes a security framework which works on a ticket based system that issues the tokens to authenticate users and validates it during their use. In the various levels of communications the concept of secret key, master key has been introduced. In the proposed framework the Trusted Authority generates the pseudo names during each communication and provides a blind signature. The framework uses the blowfish scheme for encryption and decryption process. The trusted authority traces the dishonest users and detects the frauds during communications.

The rest of this paper is organized as follows: In the next section literature work has been elaborated. The proposed security framework has been introduced in the third section. Fourth section describes the comparative study with the exiting then at last the concluding remarks are discussed in the final section.

2. RELATED WORK
To resolve the security conflicts as mentioned in the introductory part in the mesh communication system. To resolve the conflicts of anonymity it has become mandatory to use the techniques of blind signatures of payment systems [8][9][10][11]. To hide the geographical location of user the technique of pseudonym is advantageous. It doesn't rely on the central authority like trusted third party or the domain authority. This work uses the scheme of hierarchical key based signature and strictly adhered to work on the wireless communication system. Apart from these the key establishment and ticket revocation policy are also become the critical issues. The major security attacks are heavily relied on the type of protocol at the particular layer as studied in [12]. Therefore, It has become a requirement of a security framework to solve such issues in the demanding environment. The major focus of this work is based on: 1) Use of hierarchical ID-based signature policy, 2) Ticket issuing system, 3) Master key generation, 4) Technique of pseudonym, and 5) Technique of blowfish for encryption and decryption process etc.

3. PROPOSED SECURITY FRAMEWORK
This section elaborates the complete methodology and the process of proposed framework.

3.1 Preliminaries
The basic preliminaries are described as follows:

i) Policy of Anonymity: It hides the identity of legitimate client. The client is said to be anonymous if the Ticket Issuing authority cannot link the network access identity of client to his original identity.

ii) Policy of Traceability: It is used, while the ticket authority wants to trace the identity of dishonest users.

iii) Policy of Ticket-reuse: It identifies the misbehavior of a registered client while using a depleted ticket.

3.2 Process of Proposed Framework

This framework initially use a registration scheme for authentication of mesh user and identifies the basic configuration of client's system like MAC Address, IP Address, and Type of Operating system etc. for formation of network. After the authentication it generates a user ID, which is used for client authentication process. The client selects and updates the file for transmission and use the Scheme of Hierarchical ID- Based Signature. This scheme generates a master key based on the random selection of file attributes. This master key is mapped to a secret key which is converted into a Hexadecimal code so that the trusted authority can issue a token and generates a Pseudo name to hide the original Id of client. After the token generation the Blind signature is generated to send the encrypted file to the destination client. At the destination side the client use the available token and key to receive the data in a decrypted form. The complete process of proposed framework is depicted in Figure 1.

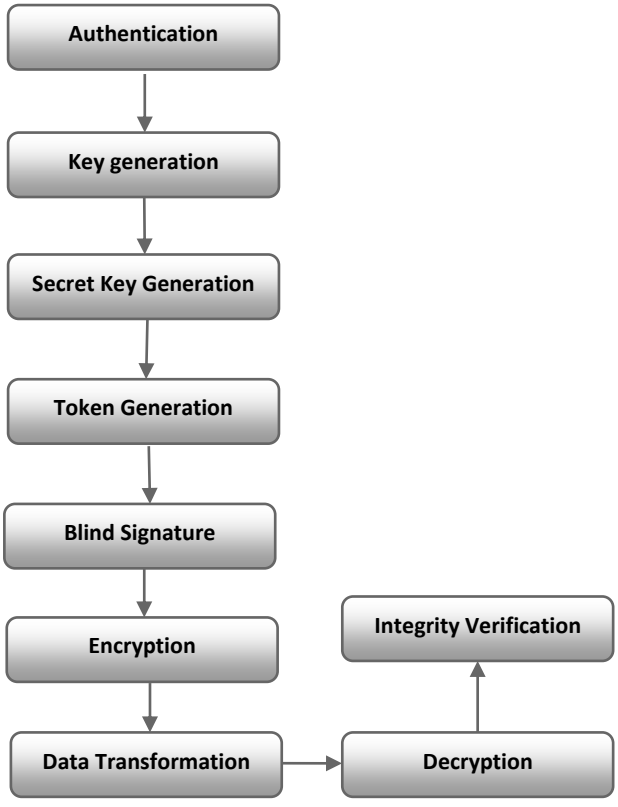

Fig 1: The Process of Proposed Framework

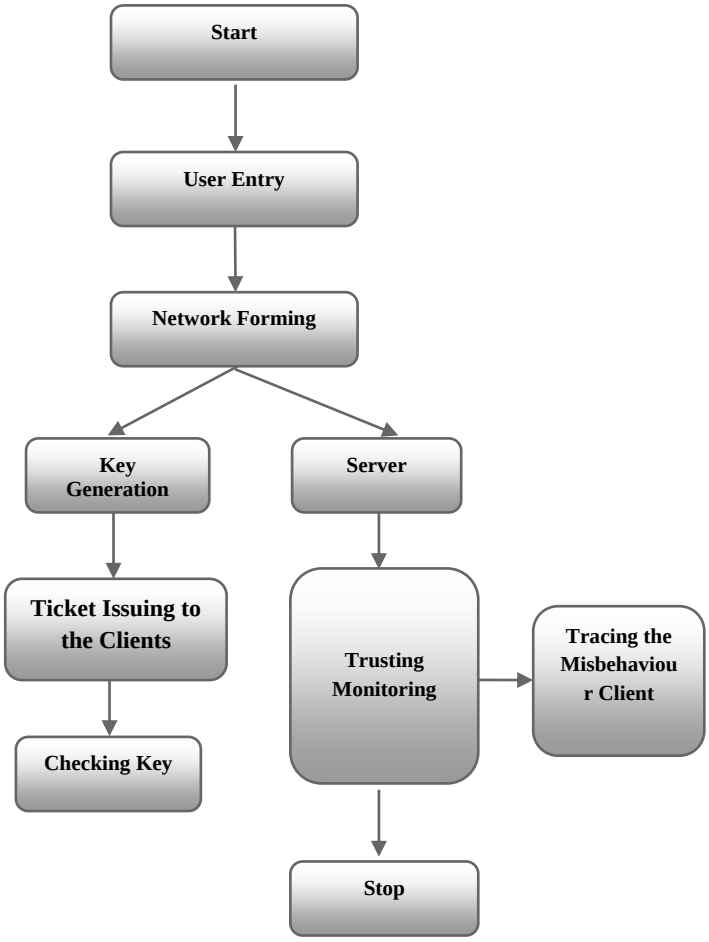

Fig 2: The Flow Diagram of Proposed Framework

3.3 Description of Modules

The flow of complete process if shown in figure 2 and the modules are described as follows:

1. User Authentication: In this phase a registration scheme is used for authentication of mesh user and identifies the basic configuration of client's system like MAC Address, IP Address, and Type of Operating system etc.

2. Formation of Network: The backbone of wireless mesh network exhibits the mesh routers and gateways that are interconnected through the wireless links. Each network is managed and controlled by a domain administrator named as the trusted authority.

2. Key Generation: This scheme generates a master key based on the random selection of file attributes. This master key is mapped to a secret key which is converted into a Hexadecimal code so that the trusted authority can issue a token and generates a Pseudo name to hide the original Id of client.

3. Generation of Blind Signature: As the name suggests, this blind signature policy is used to embed the account related information of a user into the signature of issuing bank in the encoded format. It exhibits the property of unforgeability and verifiability.

4. Ticket Issuing to the Clients: Ticket issuance occurs when the client initially attempts to access the mesh network or all the previously used tickets are completely depleted. The client is required to mention his/her original identity to the server manager so that the server manager can ensure the authenticity of the client.

5. Key Validation: It occurs when the server manager restricted the ticket requests of client because of his/her past misbehaviors. Therefore, the client is become incapable to obtain tickets from the Ticket Issuing Authority.

6. Tracing the User misbehavior: The proposed security architecture ensures the fundamental security requirements of authentication, confidentiality and data integrity. It happened because of the deployment of the basic cryptographic benchmarks.

4. COMPARATIVE STUDY WITH EXISTING PROTOCOLS

Table I: Comparative Study with the Existing Protocols Table

Protocols → / Features ↓	A-MAKE by E. Savaş et al. [13]	Who-Pay by Kai Wei et al. [9]	D. Bansal Protocol [21]	Proposed Framework
Node Registration	No	No	No	Yes
User Anonymity	No	Yes	No	Yes
Traceability	Yes	No	No	Yes
Unlinkability	Yes	Yes	Yes	Yes
Subscription Validation	Yes	No	No	Yes
Session Key Establishment	No	No	No	Yes
Hierarchical Identity Key Based Signature	No	No	No	Yes
Generation of File Attributes	No	No	No	Yes
Attribute Selection	No	No	No	Yes
Trusted Authority	Yes	No	No	Yes
Pseudo Name Generation	No	No	No	Yes
Token Generation	No	No	No	Yes
User Revocation Facility	No	No	No	Yes
Ticketing Issuance System	No	No	No	Yes
Technique of Blind Signature	No	No	No	Yes
Total Rounds for Communication	3	3	3	2
Average Key Computation Time in millisecond (In 2.8 GHz Processor with 100 samples)	NA	NA	NA	1.2
Average Token Generation Time in millisecond (In 2.8 GHz Processor with 100 samples)	NA	NA	NA	2.7

Here the security of the proposed framework is analyzed in Table 1 to verify whether the requirements mentioned in the literature have been satisfied or not

5. CONCLUSIONS AND FUTURE WORK

This work proposed a security framework mainly based on a ticket-based protocol, in which the Ticket are generated based on user past profile. This framework ensures to issue a single ticket to all the registered clients to minimize the overhead of extra storage. If the client misbehaves at any period of communication then his tickets is depleted by the Ticket Issuing Authority to ensure the traceability of dishonest users. The proposed framework achieves the fundamental security objectives and work efficiently in terms of storage as well as for communication perspective. In future this work can be enhanced to restrict the attacks like wormhole, Spoofed routing and forwarding etc.

6. REFERENCES

[1] W. Lou and Y. Fang, A Survey on Wireless Security in Mobile Ad Hoc Networks: Challenges and Possible Solutions, edited by X. Chen, X. Huang and D.-Z. Du, Kluwer Academic Publishers/Springer, 2004.

[2] L. Zhou and Z. J. Haas, “Securing ad hoc networks,” IEEE Network Magazine, vol. 13, no. 6, pp. 24–30, Dec. 1999.

[3] M. Raya and J-P. Hubaux, “Securing vehicular ad hoc networks,” Journal of Computer Security, Special Issue on Security of Ad Hoc and Sensor Networks, vol. 15, no. 1, pp. 39–68, 2007.

[4] 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.

[5] A. Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks," Comm. of the ACM, vol. 47, no. 6, pp. 53–57, 2004.

[6] 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.

[7] S. Brands, "Untraceable off-line cash in wallets with observers," in Proc. CRYPTO'93, 13th Annual Int'l Cryptology Conf. on Advances in Cyptology, pp. 302–318, Aug. 1993.

[8] K. Wei, Y. R. Chen, A. J. Smith, and B. Vo, "Whopay: A scalable and anonymous payment system for peer-to-peer environments," Proc. IEEE Intl. Conf. on Distributed Computing Systems, ICDCS, July 2006.

[9] D. Figueiredo, J. Shapiro, and D. Towsley, "Incentives to promote availability in peer-to-peer anonymity systems," in Proc. IEEE Int'l Conf. on Network Protocols, ICNP, pp. 110–121, Nov. 2005.

[10] D. Chaum, Blind signatures for untraceable payments, Advances in Cryptology - Crypto '82, pp. 199-203, Springer-Verlag, 1982.

[11] Priyanka Patel and Abhay Kothari. A Brief Review on Security and Privacy Issues in Wireless Mesh Networks. International Journal of Computer Applications 144(4):6-9, June 2016.

[12] A. O. Durahim, E. Savaş, "A-MAKE: An Efficient, Anonymous and Accountable Authentication Framework for WMNs", In the Proceedings of the 5th International Conference on Internet Monitoring and Protection (ICIMP), Barcelona, Spain, 2010, pp. 54-59.

[13] D. Bansal, S. Sofat, and A. K. Gankotiya, "Selfish MAC Misbehaviour Detection in Wireless Mesh Networks", In the Proceedings of 2010 International Conference on Advances in Computer Engineering (ACE 2010), Bangalore, Karnataka, India, 2010, pp. 130-133.