Session Key Authentication Mechanisms for Wireless Sensor Network Users

Savitha S.V [*], Jisha K [**]

[*] M.Phil Research Scholar, Sree Narayana Guru college, K.G .Chavadi, Coimbatore 6411 05
[**] M.Phil Research Scholar, Sree Narayana Guru college, K.G .Chavadi, Coimbatore 6411 05

Abstract- Seamless roaming over wireless network is highly desirable to mobile users, and security such as authentication of mobile users is challenging. Recently, due to tamper-resistance and convenience in managing a password file, some smart card based secure authentication schemes have been proposed. This paper shows some security weaknesses in those schemes. As the main contribution of this paper, a secure and light-weight authentication scheme with user anonymity is presented. It is simple to implement for mobile user since it only performs a symmetric encryption/decryption operation. Having this feature, it is more suitable for the low-power and resource-limited mobile devices. In addition, it requires four message exchanges between mobile user, foreign agent and home agent. Thus, this protocol enjoys both computation and communication efficiency as compared to the well-known authentication schemes. As a special case, we consider the authentication protocol when a user is located in his/her home network.

In this paper, we propose a privacy-preserving universal authentication protocol, called Priauth, which provides strong user anonymity against both eavesdroppers and foreign servers, session key establishment, and achieves efficiency. Most importantly, Priauth provides an efficient approach to tackle the problem of user revocation while supporting strong user untraceability**.**

I. INTRODUCTION

A privacy-preserving user authentication scheme should satisfy the following requirements [1]: (1) Server Authentication: a user is sure about the identity of the foreign server. (2) Subscription Validation: a foreign server is sure about the identity of a user's home server. (3) Provision of user revocation mechanism: due to some reasons (e.g., the subscription period of a user has expired or a user's secret key has been compromised), user authentication should allow a foreign server to find out whether a roaming user is revoked. (4) Key establishment: the user and the foreign server establish a random session key which is known only to them and is derived from contributions of both of them. In particular, the home server should not know the session key. (5) User anonymity: besides the user and its home server, no one including the foreign server can tell the identity of the user; and (6) User intractability: besides the user and its home server, no one including the foreign server is able to link any past or future protocol runs of the same user.
When user revocation is supported in an authentication protocol, it is more challenging to achieve user untraceability because on one hand, information is given to foreign servers to identify revoked users, but on the other hand, the information should not enable foreign servers to link other protocol runs of the revoked user. More specifically, the protocol runs involved by a revoked user before his revocation should remain anonymous and unlinkable. This is referred to as backward unlinkability in roaming service. In addition, for a time-limited revocation due to, for example, suspension of service for a period of time, the anonymity and the unlinkability of the revoked user's protocol runs after the revocation period should also be maintained. We refer to this property as forward unlinkability in roaming service. Requirement (6) includes backward and forward unlinkabilities which, until now, are unsolved problems.

In this paper, we assume that the attacker has total control over all communication channels among the user, foreign server and home server. That is, the attacker may intercept, insert, delete, or modify any message in the channels. Particularly, we consider four major types of threats to user authentication, namely, message en route threat, false mobile user threat, DoS attack and deposit-case attack [4]. The message en route threat includes that an attacker relays and/or redirects messages. The false mobile user threat includes the case where an attacker could impersonate a foreign/home server, as well as the case where mobile users under the control of an attacker collude. DoS attack refers to the overwhelming service requests from attackers in the purpose of blocking services from genuine mobile users. In deposit-case attack, the user is honest while there is a malicious server M, who will make the foreign server V to believe that the home server of the user is M without being detected by the user nor its home server.

In this paper, we address the problem of authentication in WSNs, particularly authenticated broadcast/multicast by sensor nodes and outside user authentication. The problem of authenticated broadcast/multicast by sensor nodes is not addressed by the existing authentication schemes for WSNs. Symmetric schemes like mTESLA and its variations proposed for base station broadcast authentication use Message Authentication Code (MAC) and are efficient in terms of processing and energy consumption.

However, they suffer from the following issues:

- Provide delayed authentication.
- Not scalable in terms of number of senders.
- Multiple senders cannot broadcast simultaneously.
- Very slow for large scale sensor networks.
- DoS attack against storage due to late authentication.
- If a sensor node wants to broadcast a message, it unicasts the message to the base station, which then broadcasts that message on behalf of that node.

This paper makes two main contributions: (1) We show some security weaknesses of current user authentication protocols in wireless communications. (2) We propose a privacy- preserving universal authentication protocol called Priauth. By introducing Verifier-Local Revocation Group Signature with Backward Unlinkability (VLR-GS-BU), it can satisfy all requirements described above. Also, Priauth only requires the roaming user and the foreign server to be involved in each protocol run, and the home server can be off-line. Additionally, Priauth belongs to the class of Universal Authentication Protocols in which same protocol and signaling flows are used regardless of the domain (home or foreign) a roaming user is visiting. This helps reducing the system complexity in practice.

Furthermore, Priauth supports verifier-local revocation, which means that verifiers (i.e., foreign servers) can, based on the revocation list (RL) sent from the home server, check locally whether a roaming user is revoked. Note that VLRGS- BU is not originally designed for authentication purpose and a direct application of it imposes two problems in Priauth. Firstly, it does not allow Priauth to support new group member joining after system setup. Secondly, it does not provide Priauth the single registration property commonly available in most existing authentication protocols, which requires a user only to register once at the home network before being able to access the global network. We will provide solutions to these two problems to make Priauth practical.

II. AUTHENTICATIONS IN WSN

Authentication in WSN can be divided into three categories, namely base station to sensor nodes, sensor nodes to other sensor nodes, and outside users to sensor nodes. The problem of authenticated broadcast by the base station has been widely addressed. We focus on the other two categories, i.e., authenticated broadcast/multicast by the sensor nodes and outside user authentication.

A. Authenticated Broadcast/Multicast by Sensor Nodes

There are many critical situations where a sensor node needs to send a quick message. For example: In a forest fire alarm application, sensor nodes deployed in a forest should immediately inform authorities about the event and the exact location of the event before the fire spreads uncontrollably. In a traffic application, whenever a sensor node senses an accident (or a traffic jam) on the road it sends an immediate message in all directions to alert other traffic approaching this location. Consider the military application scenario discussed where a troop of soldiers needs to move through a battlefield. Sensor nodes deployed there detect the presence of the enemy and broadcast this information immediately throughout the network. Soldiers, passing near these sensor nodes, use this information to strategically position themselves in the battlefield.

All these scenarios require a message to be sent as quickly as possible. Due to wireless media, transmission and reception of a message consume considerable time. Moreover, in most cases a message propagates through several hops to reach the desired destinations. Therefore, the signature generation time and the verification time should be as small as possible. A delayed message may have undesirable effects. For example, it may result in fire spreading uncontrollably and a traffic jam becoming worse. A delayed message regarding the presence of an enemy in the battlefield may cause the death of soldiers while moving through the battlefield. In all the above situations, message authentication is required otherwise a malicious entity may exploit its absence. For example, an adversary may send fake messages to block traffic towards a specific region or to turn traffic towards a specific direction. In battlefield, sensor nodes deployed by the enemy can disseminate wrong information about enemy's movement, thus deceiving soldiers. Moreover, in all the above mentioned scenarios, sensor nodes on the path from the sender node to the receiver(s) relay the messages towards destination.

Wireless communication allowing an adversary to inject false messages during multi hop forwarding causes sensor nodes to relay false data and deplete their energy. Hence, sensor nodes on the path should be able to authenticate and filter out false messages as early as possible to save relaying energy. Therefore, they are also potential receivers of these messages, arising the need of authenticated multicast by sensor nodes. In battlefield application, all sensor nodes in the network are potential receivers of critical information, arising the need of authenticated broadcast by sensor nodes. To summarize, all these scenarios require a secure mechanism which, on one hand, enables all sensor nodes in the network to send an immediate authenticated message to report a critical situation, and on the other hand, enables every receiver to verify this message.

B. User Authentication

Sensor nodes data may be confidential and in some situations only the subscribed users, who have paid, are allowed to obtain this data. A user authentication mechanism aims to prevent unauthorized users to access data from sensor nodes. Usually, a mechanism to provide an outside user access to sensor nodes data requires three tasks:

1) User Authentication allows only legitimate users of the data to access it.

2) Access Control allows a user to access only the data which he is entitled to access.

3) Session Key Establishment enables secure exchange of user queries and confidential data between users and sensor nodes.

In centralized user authentication, all users are authenticated through the base station. This mechanism is easy to deploy because the base station is a powerful device which can perform complex cryptographic operations. However, this approach has a few drawbacks. Firstly, it makes the base station a single point of failure. Secondly, it causes sensor nodes near the base station to deplete their energy quickly as for every user request; they relay packets between base station and queried sensor nodes. Furthermore, it causes a severe DoS attack where an adversary sends fake request messages causing sensor nodes to relay them towards the base station for verification, increasing network traffic and depleting their energy. User authentication schemes discussed all suffer from these problems. To avoid this kind of DoS attack, a user should be locally authenticated by the sensor nodes without the involvement of a third entity, i.e., a distributed approach.

This approach reduces traffic congestion and transmission overhead within the network. However, it puts the burden of authentication on sensor nodes. As sensor nodes are resource constrained devices as compared to the base station, a lightweight user authentication mechanism is needed for sensor nodes to verify authenticity of the users.

III. SESSION KEY ESTABLISHMENT

To provide secure transmission of data from sensor nodes to user, a session key needs to be established. For this purpose, any secure key exchange protocol could be used here. However, an identity based one-pass key establishment protocol is an attractive choice for resource constrained sensor nodes. It reduces the number of messages exchanged during key establishment phase i.e., only one party computes and sends its ephemeral key to the other party, for example, identity based one-pass key establishment protocol presented. That single message can be combined with user request message (in user authentication phase) which is signed by the user. It further reduces the communication. It also avoids the man in the-middle attack. The only message exchanged between the user U and the sensor node A for key establishment will be signed by U and verified by A, which makes it difficult for an intruder to send fake ephemeral key to the sensor nodes on behalf of U.

To establish a session key, U randomly computes its ephemeral key R. U then sends R, together with his signature, to A in authentication phase. If U's signature is valid and user authentication succeeds, both A and U compute session key SK using the key derivation function c as SK = c(IDAjjIDUjjTSjjTAU), where TS is the time stamp to avoid replayed messages and TAU is a common secret computed by both parties using R and their secret keys. At this point, the session key SK is ready for encrypting data.

User Revocation: User revocation can be divided into two cases; firstly, to revoke a user whose access time period has been expired, and secondly, to revoke a malicious user. These two cases can be treated differently. To handle the first case, at the time when base station calculates the secret key for a user U, the expiry time ET of the user can be used as a parameter to calculate the secret key. After his access time period expires, his secret key will automatically expire. If he now sends a signed request, it will not pass verification. In the second case, the base station issues an authenticated revocation list containing malicious user's ID. Sensor nodes store it until the malicious user's expiry time is passed. Thus, if next time that user attempts to access data from sensor nodes, the sensor nodes reject his request without going through authentication process. After his access time expiration, his secret key will expire and he will not be able to successfully authenticate himself to the system. In WSN, the case of the malicious users is not very common. Therefore, storing IDs of malicious users until their expiry time will not impose an unreasonable storage overhead on sensor nodes. To efficiently handle storage, user's access period can be kept short so that sensor nodes do not store malicious users' IDs for a long time. After that time period only the private keys of the legitimate users are updated for next time period. The duration of this period depends on how frequently the event of the malicious users occurs. Although some figures would help to improve the readability of framework, space limitation does not allow it.

IV. FURTHER RESEARCH SCOPE

So far the proposed authentication schemes are based on either cryptography or physical layer information. An integration of these two primitives are desirable to secure the emerging wireless networks. For example, in highly dynamic networks, such as mobile ad hoc networks, vehicular ad hoc networks, or delay tolerant networks, it is hard to maintain a central authority to efficiently distribute and manage the key. Therefore, users without any pre-established contact have to initialize a shared secret or associate to each other on-the-fly. Traditional cryptography based Diffie-Hellman key exchange technique can serve for this purpose. However, it is subject to man-in-the-middle attack. In order to prevent the man in- the-middle attack, two parties usually rely on a shared secret. Thus, it brings the dilemma that Diffie-Hellman is used to generate a shared key between two parties, but in order to prevent the man-in-the-middle attack, we need a pre-shared secret between the two parties. A possible and promising solution to this problem can be a cross-layer security design. By exploiting the unique properties of the wireless channel, the two parties can somehow identify or authenticate the message exchanged in the Diffie-Hellman protocol without relying on a preshared key. For example, Alice knows it is Bob sending the Diffie-Hellman key exchange messages to her when she observes a signal characteristic associated with these messages, and this characteristic can only be induced at a particular location where Bob is at.

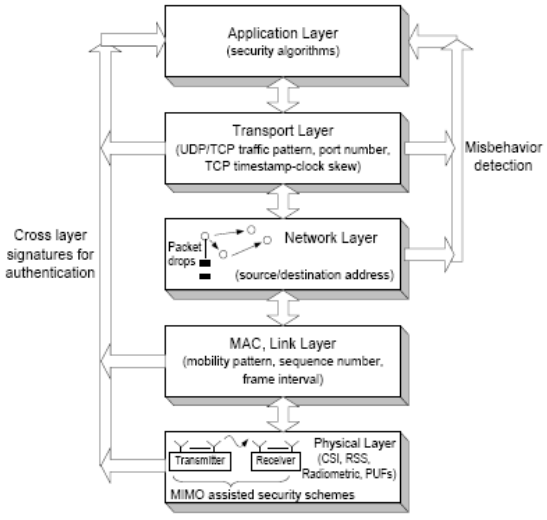

Fig. 1. Cross layer security schemes

For intrusion or malicious behavior detection, it is also desirable to examine multiple layer information to improve the probability of detection. The dependency and correlation between multiple layer behaviors or observations can be used to detect malicious/selfish nodes. An illustrative example of a cross layer signature scheme for authentication as well as misbehavior detection is given in Fig. 1. Physical layer CSI/RSS/radiometric information and emerging technologies, such as MIMO

(multiple-input and multiple output) can be combined with the MAC layer sequence number/frame interval/mobility pattern and Transport layer TCP time stamp/traffic pattern/port number to generate a strong authentication scheme to authenticate a node. For misbehavior detection, network layer source address and destination address can be used along with the transport layer traffic patterns.

V. CONCLUSIONS AND FUTURE WORK

The main contribution of this research work is to propose an authentication framework which provides two features; quick authenticated broadcast by sensor nodes and user authentication. Existing broadcast authentication schemes in WSN do not handle the problem of authenticated broadcast by sensor nodes. The proposed ID-based Online/Offline Signature (IBOOS) based broadcast authentication scheme is an attractive solution to this problem. An ID-based Signature (IBS) based distributed user authentication scheme is also proposed to authenticate outside users. Session keys secure the further communication between users and sensor nodes. The main advantage of this framework is its re-usability, that is, it can also be reused with new IBS and IBOOS schemes for security and performance improvements. In the future, we intend to focus on user access control to provide a complete ID-based authentication framework which would enable the sensor nodes, on one hand, to broadcast a message to quickly respond to some critical situations and, on the other hand, to control user access according to his access privileges. We are on the way to implement the proposed framework on real sensor nodes to get actual results. In this paper, we have proposed a novel protocol to achieve privacy-preserving universal authentication for wireless communications. The security analysis and experimental results show that the proposed approach is feasible for real applications.

REFERENCES

[1] D. He, M. Ma, Y. Zhang, C. Chen, and J. Bu, "A strong user authentication scheme with smart cards for wireless communications," Computer Commun., 2010, doi:10.1016/j.comcom.2010.02.031.

[2] G. Yang, Q. Huang, D. S. Wong, and X. Deng, "Universal authentication protocols for anonymous wireless communications," IEEE Trans. Wireless Commun., vol. 9, no. 1, pp. 168-174, 2010.

[3] G. Yang, D. S. Wong, and X. Deng, "Anonymous and authenticated key exchange for roaming networks," IEEE Trans. Wireless Commun., vol. 6, no. 9, pp. 3461-3472, 2007.

[4] G. Yang, D. Wong, and X. Deng, "Deposit-case attack against secure roaming," in Proc. ACISP'05, 2005.

[5] D. He and S. Chan, "Design and validation of an efficient authentication scheme with anonymity for roaming service in global mobility networks," Wireless Personal Commun., 2010, doi:10.1007/s11277-010- 0033-5

[6] M. Zhang and Y. Fang, "Security analysis and enhancements of 3GPP authentication and key agreement protocol," IEEE Trans. Wireless Commun., vol. 4, no. 2, pp. 734-742, 2005.

[7] C. C. Lee, M. S. Hwang, and I. E. Liao, "Security enhancement on a new authentication scheme with anonymity for wireless environments," IEEE Trans. Consumer Electron., vol. 53, no. 5, pp. 1683-1687, 2006.

[8] C. C. Wu, W. B. Lee, and W. J. Tsaur, "A secure authentication scheme with anonymity for wireless communications," IEEE Commun. Lett., vol. 12, no. 10, pp. 722-723, 2008.

[9] J.-L. Tsai, "Efficient multi-server authentication scheme based on oneway hash function without verification table," Computers & Security, vol. 27, no. 3-4, pp. 115-121, 2008.

[10] H.-C. Hsiang and W.-K. Shih, "Improvement of the secure dynamic ID based remote user authentication scheme for multi-server environment," Computer Standards & Interfaces, vol. 31, no. 6, pp. 1118-1123, 2009.

[11] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," Computer Networks, vol. 38, pp. 393–422, 2002.

[12] M. Bellare, C. Namprempre, and G. Neven, "Security proofs for identity-based identification and signature schemes," in Proc. EUROCRYPT '04. Springer-Verlag, 2004, pp. 268–286.

[13] Z. Benenson, "Realizing robust user authentication in sensor networks," in Proc. REALWSN '05, 2005.

[14] Z. Benenson, F. Gartner, and D. Kesdogan, "User authentication in sensor networks (Extended Abstract)," in Proc. Informatik 2004, Workshop on Sensor Networks, 2004.

[15] J. Bohli, A. Hessler, O. Ugus, and D. Westhoff, "A secure and resilient WSN roadside architecture for intelligent transport systems," in Proc. WiSec '08. NY, USA: ACM, 2008, pp. 161–171.

AUTHORS

First Author – Savitha S.V, M.Phil Research Scholar, Sree Narayana Guru college, K.G .Chavadi , Coimbatore 6411 05, savisudhi@gmail.com

Second Author – Jisha K, M.Phil Research Scholar, Sree Narayana Guru college, K.G .Chavadi , Coimbatore 6411 05, Jisha.unnikrishnan78@gmail.com