Evolution of Various Authentication Schemes in Wireless Network over a Decade

Pratik Singh
Department of Computer Science and Engineering,Galgotias College of Engineering & Technology, Greater Noida

Bhawna Mallick, PhD
Department of Computer Science and Engineering,Galgotias College of Engineering & Technology, Greater Noida

ABSTRACT

Openness of wireless network makes it more sensible for various security attacks. Authentication is the most vital procedure to make sure that the service is appropriately used. It is a way of confirming the genuineness of a party by another party. There is a wide range of authentication schemes that varies according to time period. This paper, focus on the authentication schemes in wireless network that have evolved in last one a decade.

Keywords

Authenticity, mesh network, roaming protocols, security attacks, handoff

1. INTRODUCTION

Security issues in wireless network are more violent due to its inadequate resources and have higher channel fault rate as compared to wired networks. Security schemes of wired network could not be used directly in wireless environment. Security is an encapsulated idea that comprises authentication, integrity, and secrecy. So authentication is habitually the primary step to set up a secure communication between two parties. Authentication means the verification of identities by a third party or two parties verify each other before participation in a transmission. So the communication between parties must be confident and secure. Authenticated parties must have trust in each other. In the absence of authentication any unauthorized user may have entrance over the channel and perform the various attacks on data such as jamming attack, impersonate attack, replay attack etc. Some data are very confidential such as military data, defense data, transaction data, economic statistics data, non-repudiation etc. Confidentiality cannot be compromised and also integrity of data needs to be maintained. Hence authentication is required to maintain confidentiality and integrity.

We consider a scenario fig.1 in wireless network there is a sender Alice, a receiver Bob and a attacker Carol, Alice transmit data to Bob but Carol perform substitution attack and modify the data on network , if receiver Bob perform authentication on received data then data will be rejected but in the absence of authentication Bob receive unmerited data. Authentication is required in every field of networks such as sensor network (WSN), mobile ad-hoc networks (MANETs), vehicular ad-hoc networks (VANETs), roaming or hand-off process, WLAN; wireless mesh networks (WMNs) etc. There are number of authentication techniques that are implemented at various layers of OSI model starting from physical layer to application layer. For example, certificates and digital signatures are present higher than the physical layer, while with an additional cost in bandwidth spread-spectrum communications is present at the physical layer usually. There are number of authentication schemes that are growing over time for every type of network. In this paper, we include studied a variety of authentication schemes in wireless network that have evolved over a decade.

The rest of the paper is organized as follows. The next section describes about the various authentication schemes that have been introduced in last one decade. Finally, in Section III we provide a conclusion of the paper and references give in the end of paper.

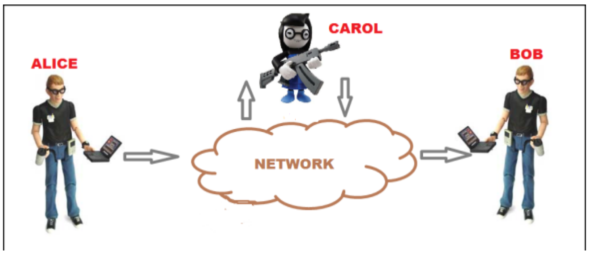

Fig.1.Proposed Scenario

2. COMPLETE STUDY OF AUTHENTICATION SCHEMES OVER A DECADE

There are ranges of authentication schemes grow up over a decade for each field of wireless network. First we consider evolution of authentication approaches in cellular network during handoff process. Jianming Zhu and JianfengMa [1], proposed a authentication Scheme with Anonymity for Wireless Environments based on hash based authentication scheme for mobile users. In this mobile user only perform symmetric encryption and decryption on message exchange. The most important characteristic of this is one time use of key linking mobile user and visited network. The security depends on tamper-proof and one way scheme. Minghui shi, Xuemin (sherman) shen, and Jon W. Mark [2], authentication approach implemented at application layer is introduced for Internet applications that are running on mobile station. It keeps the communications private to other wireless LAN users and foreign networks. In this scheme, the major authentication task is performed by the home network and finally the result is send to the mobile station.

According to Jahan Hassan, Harsha Sirisena, and Bjorn Landfeldt [7] introduced an authentication approach during handoff between access points (APs), this proposed an authentication scheme which reduced the authentication delay by nearest APs share the security key for the visiting node as the likelihood of two nearest APs trusting each other increases then complete authentications desired for a roaming mobile linearly reduces. In paper [10], Haojin Zhu, Xiaodong Lin,,Rongxing Lu, Pin-Han Ho, and Xuemin (Sherman) Shen proposed an authentication for future metropolitan-area wireless mesh networks (WMNs) with high frequency inter domain events addresses secure localized authentication and billing (SLAB) scheme (SLAB).

Mobility of a user is extremely attractive feature in wireless networks and telecommunication systems, so a user who in the beginning subscribed to their home network can be able to entrance services of cellular network without geographical limitations. There are a number of authentication techniques to authenticate mobile users by foreign network but there is no authentication server support the authentication of the foreign server by the mobile users. In paper [14], Chin-Chen Chang introduces a trusted authentication server allow both mobile user and visited foreign server to authenticate each other. Mobile users should be permitted to decide a specific foreign server to acquire the services they require. It is a self-verified mobile authentication scheme. According to GuominYang [15], there is a grim security blemish in the Key Delegation Phase of the Chang- Tsai self-verified mobile authentication scheme; mobile users can recover the long-term secret key from home server without performing any active attacks. Paper present a little different user key generation algorithm without loss in efficiency or other features.

Xiaowei Li, YuqingZhang [17], proposed a light weight roaming authentication protocol to cut the home server heavy load. Proposed authentication scheme avoid the participation of home server and take benefit of ID-based cryptography and also maintain the privacy of a user during authentication. In ID-based cryptography people can use their ID or email address as their public key. This approach have good performance in conditions of processing costs and security and applicable on Cellular Networks and Wireless Mesh Networks.

Existing system for handover describe in figure 2, mainly attention on secure authentication unit, but avoid to protecting users' confidentiality when a user verify by the entrance points to use data. Daojing He,Jiajun Bu, Sammy Chan, Chun Chen [18], proposed a authentication protocol named Handauth. Handauth support the communication efficiency and also attain well-built user ambiguity and conditional privacy-protection, forward secure user repeal, user untraceablility, access service expiration management, AAA server inscrutability, access point authentication, vibrant user revocation, easily revocation that listed, and attack confrontation. In this paper describe the twelve properties that should be satisfied by a handoff protocol. Hyo Jin Jo, Jung Ha Paik, and Dong Hoon Lee [20] proposed a three-round anonymous roaming protocol based on the signcryption scheme for authentication and avoid the participation of home server. Signcryption is a technique for encryption and create digital signature. Proposed approach used pseudo-identities that are not associated to the original identities of the roaming users.

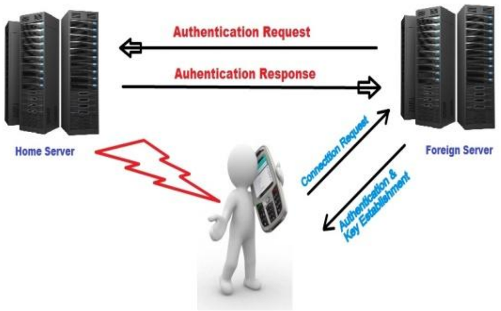

Fig.2 Handover

Table I

Sr. No.	**Paper Title**	**User Anonymity**	**Home Server Participation**	**Cryptosystem Use**	**Scalability**	**Important Feature**
1	A New Authentication Scheme with Anonymity for Wireless Environments	Yes	Yes	Symmetric public key	Low	One time use key
2	IEEE 802.11 Roaming And Authentication In Wireless Lan/Cellular Mobile Networks	No	Yes	Key agreement	Low	Support 3G
3	Trust-Based Fast Authentication for Multiowner Wireless Networks	No	Yes	Shared session key	Average	reduced the authentication delay
4	SLAB: A Secure Localized Authentication and Billing Scheme for Wireless Mesh Networks	No	Yes	Key agreement	Average	Use in metropolitan-area wireless mesh networks
5	An Anonymous and Self-Verified Mobile Authentication with Authenticated Key Agreement for Large-Scale Wireless Networks	Yes	No	Key agreement	High	Self verified
6	Comments on "An Anonymous and Self-Verified Mobile Authentication with Authenticated Key Agreement for Large-Scale Wireless Networks	Yes	No	Key agreement	High	Correction in key phase[14]
7	A Lightweight Roaming Authentication Protocol for Anonymous Wireless Communication	Yes	Yes	ID-cryptography	Average	Light weight roaming protocol
8	Handauth: Efficient Handover Authentication with Conditional Privacy for Wireless Networks	Yes	Yes	Session key establishment	Average	untraceablility
9	Efficient Privacy-Preserving Authentication in Wireless Mobile Networks	Yes	No	pseudo-identity-based signcryption	High	Home server participation reduces linearly

On the other hand, if legal issues occur, the related real identity can be used. The authentication effectiveness is also higher than that of presented protocols. In the proposed authentication protocol, both of them initially exchange trusted information that they have and result is an authenticated key that trim the roaming user and foreign sever to each other. The comparison of these authentication schemes on the basis of anonymity, scalability, home server participation, cryptosystems used, with special feature has been describe in table I.

Now, we also consider the evolution of authentication schemes in other areas of wireless networking. According to Bhargava and Mihail L. Sichitiu [3], introduced an authentication scheme that successfully defend "parking lot attack" and identify intruders based on their position. This approach relies on received signal strength (RSSI) from position. A Bayesian technique is used to guess the position of the unsuspecting mobile abuser. Zhi Li, Qibin Sun,Yong Lian and Chang Wen Chen [4] proposed approach for authenticating multimedia content delivered over heterogeneous wireless networks and also focus on security issues in multimedia transmission , also introduce a concept of called unequal authenticity protection (UAP) for protecting multimedia stream from channel noise and intrusion.

In figure 3 describe the multimedia packet authentication scheme

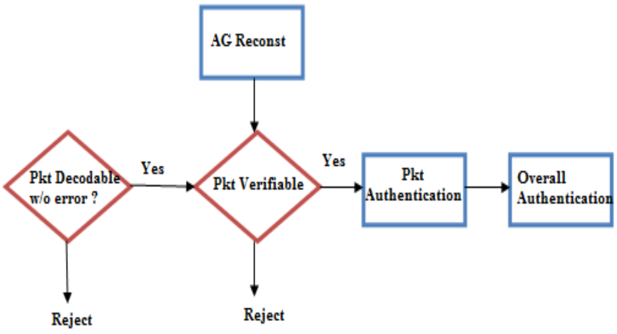

Fig. 3 Packet Authentication

Andreas Roos, Sabine Wieland,Andreas Th. Schwarzbacher,BangnanXu [5], investigate the authentication architecture of centralized, hierarchical and distributed, are presented and found that centralized authentication required least intelligence, .the distributed approach reduces the authentication path length and hierarchical authentication suited for challenging and fastest authentication.

Liang Xiao, Larry Greenstein, Narayan Mandayam [6] proposed a physical layer authentication technique based on channel probing and hypothesis testing to find out whether current and prior communication attempts by the same user .In this way, genuine users can be consistently authenticated and intruders can be consistently detected. Paul L. Yu, John S. Baras [8], proposed a physical layer authentication technique based on tag generation from a message and then generated tag send to the Bob with the message. The tag was generated by a shared key between Alice and Bob, if Bob validate the message with tag then accept message otherwise reject the message and sender both. Liang Xiao, Larry J. Greenstein, Narayan B. Mandayam, and Wade Trappe [9] describe an authentication technique based on generalized channel response with both spatial and temporal variability, variability, and reflect on correlations among the time, frequency and spatial domains. It is also based on physical layer authentication uses radio channels and hypothesis testing.

Wei Wang, Dongming Peng, Honggang Wang, Hamid Sharif, Hsiao-Hwa Chen [11] proposed a basic evolutionary algorithm for resource distribution with P-V decoding and authentication need consideration. The objective of this proposal is to optimize the honesty and quality performance gain within energy constraint. According to Wei Wang, Dongming Peng, Honggang Wang, Hamid Sharif, and Hsiao-Hwa Chen [12], propose a quality-driven scheme to optimize stream authentication and unequal error protection (UEP) jointly. This is very useful in image authentication, energy efficiency, secure and vigorous multimedia communications and provides quality of service. It will be suited for authentication in wireless mesh network. Srdjan _ Capkun, Mario _ Cagalj, Ghassan O. Karame, and Nils Ole Tippenhauer, [13], introduce integrity region authentication approach that facilitates to authenticate a party without the use of precertified keys. Ultrasonic techniques can be used to implement IRegions. It prevents from **man-in-the-middle (MITM) attacks,** if the users can confirm that the attacker is not present in their immediate locality and then users will be able to verify the reliability and the genuineness of the exchanged data and therefore check MITM attacks.

Authentication and topology control are considered separately but in MANETs they are correlated. Quansheng Guan, F. Richard Yu, Shengming Jiang, and Victor C. M. Leung, [16], jointly think about topology control and authentication both have impact on throughput. Proposed a joint authentication and topology control (JATC) scheme to pick up the throughput and examine the efficient throughput at the above layers from physical layer schemes. Jitendra K. Tugnait [19], using the unique wireless channel state information (CSI) of a user on physical layer to authenticate and avoid the intruder on the basis of CSI. It pass up the additional lumber of symbol timing harmonization and training sequence knowledge required for channel assessment.

Vehicular communication has great demand for speedy message exchanges during travel for use of multimedia services at a very high speed of up to 350 km/h. These requirements are meeting by the Worldwide interoperable for Microwave access (WiMAX) and Long-Term Evolution (LTE). WiMAX and LTE are Fourth-Generation (4G) wireless technologies that meet to the requirements of quality and security also, but there are also some issues concerns about security such as an introduction of rascal node, denial of service (DoS), etc. So, required an robust authentication schemes. Perumalraja Rengaraju, Chung-Horng Lung and Anand Srinivasan[21], proposed a security architecture for distributed network using the elliptic curve Diffie–Hellman (ECDH) protocol. It couldn't degrade the quality while enhance the security and do not use a lot of bandwidth that has low fixed cost for 4G network.

Liang Zhou, Dan Wu,Baoyu Zheng, Mohsen Guizani [22], proposed a joint framework relating both the security technologies at physical and application layer to satisfy the increasing hassle for the safety measures of wireless multimedia services. Both of the layers have considerable impact on security performance. The offered wireless set-up assets can be utilized capably by exploring the physical layer features of security and signal processing as well as certification and watermarking technique at the application layer, the joint scheme can be simply establish with low implementation cost and support deployment of wireless multimedia systems at large-scale.

As discussed earlier, in table 1 compare the various cellular network handoff authentication schemes on the basis of many factors. Jianming Zhu and JianfengMa introduce the first hand-off authentication scheme to provide user anonymity during visit to foreign network then paper[14]-[20] also follow the same concept of anonymity. Authentication scheme in [7], reduced the authentication delay and for better scalability the participation of home server for authentication has been removed by Chin-Chen Chang [14] and introduce the concept of self verification. In paper [20], introduced the latest concept of authentication based on pseudo-identity-based signcryption reduces home server participation linearly.

There are several authentications proposed schemes in various wireless areas discussed, papers [4], [11], [12], [22] deal with the authentication schemes for multimedia delivery in sensor networks or LAN network. The idea of authentication that support various authentication architectures as centralized, hierarchical and distributed has been presented by Andreas Roos, Sabine Wieland,Andreas Th. Schwarzbacher,BangnanXu [5]. Papers [3], [6], [8], [9], [19] presented physical layer authentication approaches. For MANETs [16], a joint authentication and topology control (JATC) scheme was proposed with improvement in throughput of network improve the throughput Perumalraja Rengaraju, Chung-Horng Lung and Anand Srinivasan [21], introduced the vehicular authentication that support 4G networks up to 350 km/h for multimedia applications.

3. CONCLUSION

In this paper, we studied the various authentication schemes that have evolved over a decade. They cater to the requirements of authentication in different areas of wireless networks. In table 1, we compared the various proposed cellular network authentication schemes during hand-off process based on scalability, anonymity etc. and also addressed the authentication schemes of other areas in wireless networks at various layers of OSI model such as in mesh networks, sensor networks, vehicular communication etc. these authentication schemes not only provide the authentication as well as also provide the additional security from a variety of threats.

4. REFERENCES

[1] Jianming Zhu and JianfengMa,"A New Authentication Scheme with Anonymity for Wireless Environments",IEEE Transactions on Consumer Electronics, 234 Vol. 50, No. 1, February 2004.

[2] Minghui shi, Xuemin (sherman) shen, and Jon W. Mark, University of waterloo, "IEEE 802.11 Roaming and Authentication in Wireless Lan/Cellular Mobile Networks”, IEEE Wireless Communications, August 2004.

[3] Vishal Bhargava and Mihail L. Sichitiu,"Physical Authentication through Localization in Wireless Local Area Networks",IEEEGlobecom 2005.

[4] Zhi Li, Qibin Sun,Yong Lian and Chang Wen Chen, Fellow, “Joint Source-Channel Authentication Resource Allocation and Unequal Authenticity Protection for Multimedia Over Wireless Networks” IEEE Transactions on multimedia, vol. 9, no. 4, June 2007.

[5] Andreas Roos, Sabine Wieland,Andreas Th. Schwarzbacher,BangnanXu,"Time behavior and network encumbrance due to authentication in wireless mesh acess networks",IEEE 2007.

[6] Liang Xiao, Larry Greenstein, Narayan Mandayam, Wade Trappe,"Fingerprints in the Ether: Using the Physical Layer for Wireless Authentication",IEEE Communications Society ICC 2007.

[7] Jahan Hassan, Harsha Sirisena, and Bjorn Landfeldt, “Trust-Based Fast Authentication for Multiowner Wireless Networks”, IEEE Transactions on Mobile Computing, Vol. 7, No. 2, February 2008.

[8] Paul L. Yu, John S. Baras,"Physical-Layer Authentication",IEEE Transactions on Information Forensics and Security, Vol. 3, No. 1, March 2008.

[9] Liang Xiao, Larry J. Greenstein, Narayan B. Mandayam, and Wade Trappe,” Using the Physical Layer for Wireless Authentication in Time-Variant Channels”, IEEE Transactions on Wireless Communications, Vol. 7, No. 7, July 2008.

[10] Haojin Zhu, Xiaodong Lin,,Rongxing Lu, Pin-Han Ho, and Xuemin (Sherman) Shen,“ SLAB: A Secure Localized Authentication and Billing Scheme for Wireless Mesh Networks”, IEEE Transactions on Wireless Communications, Vol. 7, No. 10, October 2008.

[11] Wei Wang, Dongming Peng, Honggang Wang, Hamid Sharif, Hsiao-Hwa Chen,” Matching Stream Authentication and Resource Allocation to Multimedia Codec Dependency with Position-Value Partitioning in Wireless Multimedia Sensor Networks” IEEE "GLOBECOM" 2009 proceedings

[12] Wei Wang, Dongming Peng, Honggang Wang, Hamid Sharif, and Hsiao-Hwa Chen,”A Multimedia Quality-Driven Network Resource Management Architecture for Wireless Sensor Networks With Stream Authentication”, IEEE Transactions on Multimedia, Vol. 12, No. 5, August 2010.

[13] Srdjan _ Capkun, Mario _ Cagalj, Ghassan O. Karame, and Nils Ole Tippenhauer, “Integrity Regions: Authentication through Presence in Wireless Networks”, IEEE Transactions on Mobile Computing, Vol. 9, No. 11, November 2010.

[14] Chin-Chen Chang,"An Anonymous and Self-Verified Mobile Authentication with Authenticated Key Agreement for Large-Scale Wireless Networks",IEEE Transactions on Wireless Communications, Vol. 9, no. 11, November 2010.

[15] GuominYang,"Comments on “An Anonymous and Self-Verified Mobile Authentication with Authenticated Key Agreement for Large-Scale Wireless Networks”IEEE Transactions on Wireless Communications, Vol. 10, No. 6, June 2011.

[16] Quansheng Guan, F. Richard Yu, Shengming Jiang, and Victor C. M. Leung, “Joint Topology Control and Authentication Design in Mobile Ad Hoc Networks With Cooperative Communications”, IEEE Transactions on Vehicular Technology, Vol. 61, No. 6, July 2012.

[17] Xiaowei Li, YuqingZhang,"A Lightweight Roaming Authentication Protocol for Anonymous Wireless Communication",Globecom 2012 - Communication and Information System Security Symposium IEEE 2012.

[18] Daojing He,Jiajun Bu, Sammy Chan, Chun Chen, "Handauth: Efficient Handover Authentication with Conditional Privacy for Wireless Networks", IEEE Transactions on Computers, Vol. 62, No. 3, March 2013

[19] Jitendra K. Tugnait,"Wireless User Authentication via Comparison of Power Spectral Densities",IEEE Journal on Selected Areas in Communications, Vol. 31, No. 9, September 2013.

[20] Hyo Jin Jo, Jung Ha Paik, and Dong Hoon Lee, "Efficient Privacy-Preserving Authentication in Wireless Mobile Networks", IEEE Transactions on Mobile Computing, Vol. 13, No. 7, July 2014.

[21] Perumalraja Rengaraju, Chung-Horng Lung and Anand Srinivasan,"QoS-Aware Distributed Security Architecture for 4G Multihop Wireless Networks", IEEE Transactions on Vehicular Technology, Vol. 63, No. 6, July 2014.

[22] Liang Zhou, Dan Wu,Baoyu Zheng, Mohsen Guizani, "Joint Physical-Application Layer Security for Wireless Multimedia Delivery", IEEE Communications Magazine • March 2014