A Secure Zero Knowledge Authentication Protocol for Wireless (Mobile) Ad-Hoc Networks

Atul Chaturvedi
Department of Mathematics
PSIT (Kanpur), India

Neelam Srivastava
Department of Electronics and Communication
IET (Lucknow), India

Varun Shukla
Department of Electronics and Communication
PSIT (Kanpur), India

S.P. Tripathi
Department of Computer Science
IET (Lucknow), India

Manoj Kumar Misra
Department of Computer Science
PSIT (Kanpur), India

ABSTRACT
Entity authentication and key distribution are very important cryptographic problems in mobile communication or in ad-hoc networks or in wireless communication at large. Mutual entity authentication is seen as the necessary process to the establishment of a secure and authentic connection. For a reliable secure communication, mutual entity authentication is very often seen as the necessity to the establishment of a secure connection. Authentication is necessary in wireless communication such as GSM or for Ad-Hoc purposes [26].Here Latin word ad-hoc means for the specific purpose only. Authentication is also necessary in situations where we need more than two entities in the authentication exchange such as a mobile user, a local AAA (Authentication, Authorization and Accounting) server and a remote (home) AAA server [8,21]. In such situations it is essential to include authentic and secure key exchange mechanism that ensures enhancement of trust in communication. This paper provides an authenticated zero knowledge protocol which is very helpful in establishing secure wireless communication in ad-hoc networks by satisfying cryptographic goals such as authentication, data integrity etc [13].

Keywords
Authentication, Wireless Communication, Ad-Hoc Networks, Secure Communication, Zero Knowledge (ZK) Protocol

1. INTRODUCTION
Authentication is an important application in the field of public key cryptography. The essence of public key authentication was introduced in 1976 by W. Diffie and M.Hellman [6]. In their seminal scheme each user gets a pair of keys, one called the public key and the other called the private key. Each user's public key is published while the private key is kept secret. The requirement of sharing secret information by sender and receiver is eliminated. So the communication involves only public keys, and no private key is ever transmitted or shared. Now it is not necessary to trust communication channel to be secure against eavesdropping or betrayal. The only requirement is that public keys must be associated with their users in a trusted (authenticated) manner (for instance, in a trusted directory). Anyone can send a confidential message by just using public information, but the message can only be decrypted with a private key, which is in the sole possession of the intended recipient. In the introduction part, for better understanding it is essential to define some terms. Entity authentication is the process which gives assurance to one party about the second party in the particular communication protocol [13]. There are specific cases where a protocol simultaneously provides entity authentication (unilateral or mutual) and session key establishment, where this session key is used to protect data. Key establishment is a process in a protocol which has a shared secret and it becomes available to two or more parties for encryption. Key authentication (sometimes also called implicit key authentication) is the property in which one party is assured that no other party aside from a specifically identified second party (and possibly additional identified trusted parties) may gain access to a particular secret key. Key confirmation is the property whereby one party is assured that a second party actually has possession of a particular secret key. Explicit key authentication is the property obtained when both (implicit) key authentication and key confirmation hold.

Key freshness or key newness are important terms and it means that the party involved in a key establishment process knows that the key is a new key or not used previously. In particular, the party should have evidence that the messages received during the protocol by which the key has been established are fresh messages, i.e. they are not replays of old messages from a previous instance of the protocol. On a general note, Authentication is a process by which a communication system or wireless communication system verifies the identity of a user who wishes to access in order to achieve access control. So authentication is must for secure communication. Sometimes, depending upon the requirement, a Trusted Third Party (TTP) may be involved as part of the authentication protocol. A Trusted Third Party is an entity that is mutually trusted and that can facilitate mutual authentication between the two parties.

An authentication protocol is a sequence of message exchanges between entities (supplicant(s) and authenticator(s)) that either distributes secrets to some of those principals or allows the use of some secret to be recognized. A credential is an identifier that can be used to

authenticate a supplicant with high confidence. An entity, be it a supplicant or authenticator, may be any of the following:

- *Peer*: It can be any person like an employee needs authorization to use resources in an email service. It can be a college email service for its employees.
- *Service*: The service can be an online financial transaction system provided by the Bank so authentication is desired for granting access.
- *Node* and *Group*: A node usually refers to a computing device that is connected to the network. Networks can have tens, thousands, or even millions of nodes. Laptops, personal digital assistants (PDA), sensors, and personal computers (PC) are all examples of nodes. A group is a collection of nodes. The example of group can be a connected network of members working over an operating system.
- *Agent*: An agent is a program that regularly performs some service in a regular interval. In this case the urgent participation of user is not essential.

Authentication is required in various applications such as cellular telephony etc [14,15,17]. The entity authentication technique may be classified into three premier categories depending upon the security and its type.

- *When something is known*: The example of this category is standard PIN (Personnel identification Number). In this case, we have secret keys whose knowledge is demonstrated in the particular challenge response protocols.
- *When something possessed*: In this category we have magnetic-stripped card, chip cards or plastic cards such as credit cards, smart cards etc which contains user's information.
- *When Something Inherent*: The purpose of mentioning this category is limited to classification point of view only because these techniques are non-cryptographic. It includes human physical characteristics such as biometrics, fingerprint recognition etc.

2. AUTHENTICATION IN WIRELESS (AD-HOC) NETWORKS

Wireless ad-hoc networks are adopted for specific purposes because they are not dependent on any pre defined infrastructure that means ad-hoc network contains individual communicating devices interacting with each other[1,2,3,4]. The simplicity and the strength can be understood by the fact that one can develop his or her own ad-hoc network in order to communicate for a particular time [22,23].The military tactical and other security sensitive operations are still main applications of ad-hoc networks. The authors named it military ad-hoc networks, although there is a trend to adopt ad-hoc networks for commercial use due to their unique properties and ease of usage [30, 31,32].

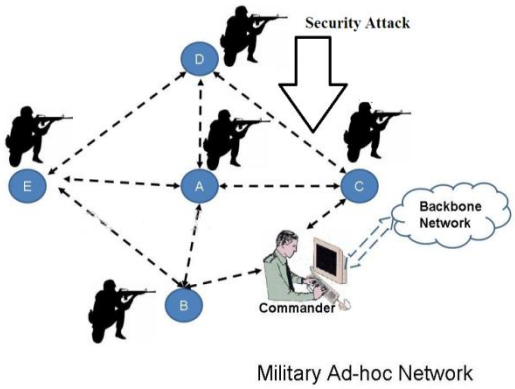

Figure 1: military ad-hoc network

Figure 1: Showing military ad-hoc network in which soldiers are communicating with each other and vulnerable to security attack.Recently many authentication protocols have been proposed for Ad-hoc networks [1,5,7,9,10,16]. For example, the IETF PANA (Protocol for carrying authentication for network access) runs under the standard of RFC 5191 (in may 2008). It was about the general layout for the transfer of authentication messages. There is a need of discussing security issues separately.The hierarchial structure of communication protocols tells that the Transport Layer Security (TLS) including Secure Socket Layer (SSL) protocols are utilizing the strength of asymmetric cryptography and authentication processes [27,28,29]. A client server model can be utilized to develop protocols other than TLS and SSL [18,19,20]. When communication begins, say client transmits a message to the intended server, the entire process must be authenticated [11]. After the authentication, they can exchange secret or session keys for communication [10,11,12]. So there is an essence of developing an authentication scheme to avoid failure of any cryptographic goal [13,24,25].

Transport layer [SSH-TRANS] Cryptographic goals: Authentication, Privacy, Integrity
User Authentication Protocol [SSH-USERAUTH] Client Authentication runs over transport layer protocol
Connection protocol [SSH-CONNECT] Multiplexes the encrypted tunnel into many logical channels. It runs over the user authentication protocol
TCP
IP

Figure 2: Layered hierarchy of Protocols and Authentication

3. PROPOSED PROTOCOL

A drawback of simple password protocol which is applicable in an ad-hoc network is that there is a chance of impersonation . Zero-knowledge (ZK) protocols are purposely designed to solve this issue. Here a sender needs to demonstrate knowledge of a secret while revealing no information whatsoever (beyond what the verifier was able to deduce prior to the protocol run) of use to the verifier in conveying this demonstration of knowledge to others. It can be said that ZK protocols allow a proof of the truth of an assertion, while conveying no information whatsoever.

Key Generation

Let g be a generator of the group Z_p^* , p is large prime. This parameter is publicly known. Sender Alice, say A and receiver Bob, say B chooses two integer a and b between 2 and p -1 respectively. A and B computes g^a and g^b and interchanges these values to each other. Here, Sender A and receiver B represents participants communicating with each other in an ad-hoc network like in the case of military ad-hoc network mentioned above. There are two parts in the defining of parameters step and they are as follows:

- A computes $k_{AB} = (g^b)^a$ and B computes $k_{BA} = (g^a)^b$ and they agree upon a common secret $k = k_{AB} = k_{BA}$. Here it is important to mention that if $k = 0$ or $k = 1$, then the entire procedure needs to repeat itself.
- A choose c between 2 and p-2, Computes $Y_A = k^C$. Thus A's public key is y_A and private key is c.

Authentication

The transfer and computation take place between the two parties which is stated below in two parts.

- B chooses random d between 2 and p-2 and sends the challenge $x = k^d$ to A.
- A sends the response $y = h(x^c)$ to B and B checks $y = H(y_A^d)$

Security Analysis

The vulnerability of the stated authentication protocol can be determined by the security analysis which is segregated into different parts.

Completeness: If A transmits y' instead of y at step 2 then the condition that B accepts incoming key depends if and only if we have $y' = H(y_A^d)$ which is $y' = H(g^{abcd}) = y$

Soundness: Suppose an intruder Eve (let's say E) is accepted in the ongoing communication with non-negligible probability. This means that E can compute $H(y_A^d)$ with non-negligible probability. As H is supposed to be an ideal hash function, this means that E can compute a number z satisfying $H(z) = H(y_A^d)$ with non-negligible probability. There are two possibilities: either we have $z = y_A^d$ which contradicts the hypothesis that DLP in Z_p is hard, or $z \neq y_A^d$ which means E and B are able to find a collision for H, contradicts the hypothesis that H is collision free.

Honest-verifier zero knowledge: In the modern world there is a huge demand of electronic transactions that can be done with ad-hoc networks and for this we need fast and cost effective key distribution system that is essential for communication of ad-hoc networks like in e- commerce and for secure money transaction schemes [12]. The zero-knowledge authentication scheme is authentication scheme which gives no knowledge beyond the authenticity. Consider the probabilistic tuning machine defined as follows: It randomly selects integer d using the same drawing as the honest verifier, and calculates the instances $(d, h(y_A^d))$. Then, the instances generated by this simulator follow the same probability distribution as the ones generated by the interactive pair (A, B).

4. CONCLUSION & FUTURE SCOPE

The preparation of a secure zero knowledge authentication scheme enhances the security level of wireless ad hoc network which ultimately satisfies all cryptographic goals. Cryptography has the strength to address security issues of Ad-hoc networks. The future scope lies in the fact that they can be very useful in other then military environment such as various commercial purposes keeping the fact in mind that ad-hoc networks do not require any pre existing infrastructure hence they are convenient to use. The related protocol environment can be developed for different situations like Electronic Health Record systems etc.

5. REFERENCES

[1] D. Balfanz, D. K. Smetters, P. Stewart, H. Chi. Wong,"Talking to Strangers: Authentication in Ad-Hoc Wireless Networks." In Symposium on Network and Distributed Systems Security (NDSS '02), San Diego, CA,2002.

[2] S. Basagni , K. Herrin,E.Rosti, D.Bruschi "Secure pebblenets." In Proc. Of the 2nd ACM international symposium on Mobile ad hoc networking & computing, 2001.

[3] M. Bechler, H.J.Hof, D. Kraft, E. Phalke, L. Wolf "A Cluster-Based Security Architecture for Ad Hoc Networks" INFOCOM 2004.

[4] J. Binder, H.P. Bischof, "Zero knowledge proofs of identity for ad hoc wireless networks." 2003.

[5] H. Deng, A. Mukherjee, D. P. Agrawal, "Threshold and Identity-Based Key Management and Authentication for Wireless Ad Hoc Networks." International Conference on Information Technology: Coding and Computing (ITCC'04), volume 1, pp 124-128.

[6] W.Diffie, & M.Hellman, New directions in cryptography, IEEE Trans. Inform. Theory,22(6),1976,644-654.

[7] W. Du, R.Wang, P. Ning, "An Efficient Scheme for Authenticating Public Keys in Sensor Networks." In Proc. of 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc), 2005.a

[8] A. Fritz , J.F. Paris, "Maille Authentication: A Novel Protocol for Distributed Authentication." In Proc. of the 19th IFIP Information Security Conference (SEC 2004), Toulouse, France, Aug. 2004, pp 309–322.

[9] S. Gokhale, P. Dasgupta, "Distributed Authentication for Peer-to-Peer Networks", In Symposium on Applications and the Internet Workshops 2003 (SAINT'03 Workshops).

[10] S. Hahm, Y. Jung, S. Yi, Y. Song, I. Chong, , K. Lim, "A Self-organized Authentication Architecture in Mobile Ad-hoc Networks." International Conference on Information Networking (ICOIN) 2005.

[11] IEEE Std 802.11a-1999 Supplement to IEEE standard for information technology telecommunications and

information exchange between systems - local and metropolitan area networks - specific requirements. Part 11: wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: high-speed physical layer in the 5 GHz band.

[12] H. Luo, P. Zerfos, J. Kong, S. Lu, , L. Zhang, "Self-Securing Ad Hoc Wireless Networks." In Seventh IEEE Symposium on Computers and Communications (ISCC '02), 2002.

[13] A.J. Menezes, P.C.V. Oorschot,, S.A.Vanstone, Handbook of Applied Cryptography. CRC Press, Boca Raton (1997)

[14] C.J. Mitchell, : Making serial number based authentication robust against loss of state. ACM SIGOPS Operating Systems Review, Volume 34, Issue 3, July 2000,pp 56–59.

[15] C.J. Mitchell, : The security of the GSM air interface protocol. Technical Report RHUL-MA-2001-3, Mathematics Department, Royal Holloway, University of London, Egham, Surrey TW20 0EX, UK (2001) Available at http://www.ma.rhul.ac.uk/techreports.

[16] E. C. H. Ngai, M. R. Lyu, "Trust- and Clustering based Authentication Services in Mobile Ad Hoc Networks." In Proc. of 24th International Conference on Distributed Computing Systems Workshops - W4: MDC (ICDCSW'04).

[17] E. C. H. Ngai , M. R. Lyu , R. T. Chin, "An Authentication Service Against Dishonest Users in Mobile Ad Hoc Networks." In Proc. of 2004 IEEE Aerospace Conference, March 6-13 2004.

[18] D. Park, C. Boyd, E. Dawson. "Classification of Authentication Protocols: A Practical Approach." Proceedings of the Third International Workshop on Information Security.

[19] A. Perrig, R. Canetti, J. Tygar, D. Song, "Efficient authentication and signing of multicast streams over lossy channels." In Proc. of IEEE Symposium on Security and Privacy, May 2000.

[20] A Perrig, R. Szewczyk, V. Wen, D. Culler, J.D. Tygar, "SPINS: Security Protocols for Sensor Networks." In Proc. Of ACM Mobicom'01, Rome, ACM Press 2001, pp 189-199.

[21] A. Pirzada, C. McDonald, "Kerberos Assisted Authentication in Mobile Ad hoc Networks." Proceedings of the 27th conference on Australasian computer science.

[22] F. Stajano , R. Anderson, "The Resurrecting Duckling: Security Issues in Ad-Hoc Wireless Networks." In M. Roe B. Christianson, B. Crispo, editor, Security Protocols, 7th International Workshop Proceedings, LectureNotes in Computer Science. Springer Verlag, 1999.

[23] R.J.Sutton : Secure communications: Applications and management. John Wiley & Sons (2002).

[24] M. Tamer Refaei, V. Srivastava, L. DaSilva, M. Eltoweissy "A Reputation-based mechanism for Isolating Selfish Nodes in Ad Hoc networks". In Proc. of the IEEE Mobiquitous 2005, San Diego, CA.

[25] L. Venkatraman, D.P. Agrawal, "A Novel Authentication Scheme for Ad Hoc Networks." In IEEE Wireless Communications and Networking Conference (WCNC 2000), vol. 3, pp 1268 -1273, 2000.

[26] M.Walker, T.Wright,: Security. In F.Hillebrand, editor.: GSM and UMTS: The creation of global mobile communication. John Wiley & Sons (2002) pp 385–406.

[27] A. Weimerskirch ,G. Thonet, "A Distributed Light-Weight Authentication Model for Ad-hoc Networks." In Proc. of 4th International Conference on Information Security and Cryptology (ICISC 2001), 6-7 December 2001.

[28] A. Weirmerskirch , D. Westhoff, "Identity Certified Authentication for Ad-hoc Networks." In Proc. of the 1st ACM workshop on Security of ad hoc and sensor networks, 2003, VA USA.

[29] R. Yahalom, B. Klein, T. Beth, "Trust Relationships in Secure Systems- A Distributed Authentication Perspective." In Proc. of the 1993 IEEE Symposium on Security and Privacy, CA USA.

[30] L. Zhou ,Z.J. Haas, "Securing Ad Hoc Networks." IEEE Network Journal, vol. 13, no. 6,1999, pp. 24-30.

[31] S. Zhu, S. Setia and S. Jajodia, "LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks." In 10th ACM Conference on Computer and Communications Security (CCS '03).

[32] S. Zhu, S. Xu, S. Setia and S. Jajodia, "LHAP: A lightweight hop-by-hop authentication protocol for ad-hoc networks." In Proc. of ICDCS 2003 International Workshop on Mobile and Wireless Network (MWN 2003), May 2003.