

A Secure Crypt Analysis of Password Authenticated Key Exchange Methodology in Wireless Sensor Network

R. Sharmila

Department of Computer Science & Engineering
Bharathidasan University, Trichirappalli, India

Abstract— Wireless sensor networks are one of the most exciting then challenging research domains of our time. They have a great potential to be deployed now wide mission-critical applications, such as military monitoring, health care as well as civilian applications. The highly sensitive nature of gathered information makes security in these special networks a crucial concern. Owing to the hostile nature of their deployment environments, the wireless medium and the constrained nature of resources on the diminutive sensor devices used in such networks, security poses more severe challenges compared to the traditional networks. As per attacks to any part of the hardware or software may give significant damages to these networks. Actually, the development of effective and efficient defense mechanisms to those attacks must be addressed at every stage of the system design. We propose Rumor Riding (RR), a lightweight and non-path-based mutual anonymity protocol for decentralized P2P systems. Employing a random walk mechanism, RR proceeds advantage of lower overhead by mainly using the symmetric cryptographic algorithm. The proposed protocols security, simplicity, and speed make it ideal for a wide range of real-world applications now which secure password authentication is required.

Key words: Authentication, Cryptanalysis, Password-Authenticated Key Agreement, Cross Domain

I. INTRODUCTION

Security is one of the main issues concerning today's networked systems. For protecting systems against malicious attacks, there occur intrusion detection systems (IDSs) and vulnerability scanners. Those solutions, however, usually identify vulnerabilities in separation, which only provides a partial picture about securing a network. Intruders are able to attack a network using multi-step intrusions. Attackers can associate individual attacks by manipulating low-level vulnerabilities to generate an attack scenario, and then achieve his/her desired critical resources inside the network.

The password-authenticated key agreement protocol is a popular method for achieving user authentication and secure communications due to its simplicity and convenience [1,2]. The Most passwords authenticated key agreement protocols are based on the single-server model [3]. This model assumed that each client had a secret password shared with a common server. However, with the emergence of a variety of complex communication environments such as global network, which has been widely deployed in a wide area of applications, which includes supply chain management, retail, security and healthcare, one of main concerns is to establish a secure channel between clients who registered in different servers.

Our proposed approach is to efficiently find a set of initial conditions in the attack graph that comprises an actionable solution for the administrator during hardening

the network. We propose a heuristic algorithm to calculate the sum of cost of initial conditions that needs to be disabled. In this study different heuristics in finding a non-optimal but good solution in reasonable time. It first present a heuristic approach based upon the relationship between cost and the number of edges. We show that these combinations can be used to find a good set of initial conditions to disable. We experimentally compare our solution with the optimal solution in terms of the resulted cost and the time taken in calculating the result.

II. REVIEW OF LITERATURE

A. An Enhanced Two-factor User Authentication Scheme in Wireless Sensor Networks

Designing user authentication protocol for wireless sensor networks is a difficult task because wireless networks are vulnerable to attacks and sensor node has limited energy, processing and storage resources. Recently, several authentication schemes have been proposed. This paper shows some of the security problems and design weaknesses in those schemes. Further, an enhanced two-factor user authentication protocol is presented. The proposed scheme only uses hash function, and a successful user authentication requires three message exchanges. Security and performance analyses demonstrate that related to the well-known authentication schemes, our proposal is more secure and efficient.

B. Cryptanalysis and Security Improvements of 'Two-Factor User Authentication in Wireless Sensor Networks'

User authentication in wireless sensor networks (WSN) be a critical security issue due to their unattended and hostile deployment in the field. Subsequently sensor nodes are equipped with limited computing power, storage, and communication modules; authenticating remote users in such as resource-constrained environments is a paramount security concern. Recently, M.L. Das proposed two-factor user authentication scheme in WSNs and claimed that his scheme is secure against different kinds of attack. However, in this paper, we show that the M.L. Das-scheme has some critical security pitfalls and cannot be endorsed for real applications. We point out that in his scheme: users cannot change/update their passwords, it does not afford mutual authentication between gateway node and sensor node, and invulnerable to gateway node bypassing attack and privileged-insider attack. To overcome the in MANET security weaknesses of the M.L. Das-scheme, we propose improvements and security patches that attempt to fix the predispositions of his scheme. The proposed security improvements can be incorporated in the M.L. Das-scheme for achieving a further secure and robust two-factor user authentication in WSNs.

C. Secured Authentication Protocol for Wireless Sensor Networks Using Elliptic Curves Cryptography

User authentication is a crucial ministrations in wireless sensor networks (WSNs) that is becoming increasingly common in WSNs since wireless sensor nodes are typically positioned in an unattended environment, leaving them open to possible hostile network attack. Since wireless sensor nodes are limited in computing power, data storage and communication capabilities, any user authentication protocol must be premeditated to operate efficiently in a resource constrained environment. In this paper, we analysis several proposed WSN user authentication protocols, with a detailed review of the M.L Das protocol and a cryptanalysis of D as' protocol that shows several security weaknesses. Furthermore, this paper proposes an ECC-based user authentication protocol that determines these weaknesses. According to our analysis of security of the ECC-based protocol, it is appropriate for applications with higher security requirements. Finally, we present a comparison of security, computation, and communication costs and recital for the proposed protocols. The ECC-based protocol is shown to be suitable for higher security WSNs.

D. A Robust Mutual Authentication Protocol for Wireless Sensor Networks

Authentication is an important service in wireless sensor networks (WSNs) for an unattended environment. Recently, Das proposed a hash-based authentication protocol for WSNs, which provides more security against the masquerade, stolen-verifier, replay, and guessing attacks and aevades the threat which comes with having many logged-in users with the same login-id. In this paper, we point out one security weakness of D as' protocol in mutual authentication for WSN's preservation between users, gateway-node, then sensor nodes. To remedy the problem, this paper provides a secrecy improvement over Das' protocol to ensure that a legal user can exercise an WSN in an insecure environment. Furthermore, by presenting the comparisons of security, computation besides communication costs, and performances with the related protocols, the proposed protocol remains shown to be suitable for higher security WSNs.

E. An Improved Remote User Authentication Scheme with Elliptic Curve Cryptography and Smart Card without using Bilinear Pairings

Login to the remote server over unpredictable insecure network demands secured password a secured password authentication using less computational cost. We have proposed a remote user authentication scheme based on ECC that establish strong authentication with key agreement. As per the password verifier table is vulnerable to security attacks and the bilinear pairing conquers more computation time, the proposed scheme avoids the usage of both, but is improved with the utility of smart card and ECC. The gathering and performance efficiency of our scheme was analyzed and proved to provide a strong mutual authentication among user and server when compared with the existing methods.

III. PROTOCOL ANALYSIS

A. Review of RR Protocol

RR protocol proceeds with 7 steps as follows:

- 1) Client A chooses random values $a, m, k \in \mathbb{Z}^*p$, computes $XA = (VA)a \oplus vA$, $EA = \{IDA, IDB, XA, m, k\}vA$ to Server SA.
- 2) Server SA decrypts EA with the stored verifier VA. Then SA computes $Em = \{IDA, IDB\} m$ and generates Ticket $B = \{IDA, IDB, IDS, k, (VA)a, L\}k$. Finally, SA sends EmandTicketB to A.
- 3) Client A checks IDA and IDB, and then sends IDA, IDB, SA ID and TicketB to client B.
- 4) Client B chooses random values $n \in \mathbb{Z}^*p$, computes $EB = \{IDA, IDB, n\}VB$ n and sends EB to Server SB with the received messages.
- 5) Server SB decrypts EB and TicketB respectively. Then, SB computes $XSB = (VA)a \oplus vB$ and $En = \{IDA, IDB, XSB, k\}n$. Finally, SB sends Ento client B.
- 6) Client B decrypts the message En, then B chooses a random value $b \in \mathbb{Z}^*p$, computes $XB = (XSB \oplus VB)h = (VA)ab$. Finally, client B sends $EKB = \{IDA, IDB, XB, (VB) b\}$ to client A.
- 7) After receiving the message from client B, A generates the session key $kAB = ((VA)ab)tA - 1 = gab$. Then, A sends $EKA = \{IDA, IDB, (VB) ab\}$ to B. Upon receiving the message, B also computes the session key $kBA = ((VB)ab)ts - 1 = gab$.

Our protocol is secure against server compromise attack. If the password file of server SA is compromised, the adversary gets vA and posing as client A. The adversary do not know tA, cannot pass the verification in Step 3.

IV. RESULTS AND DISCUSSION

A. Simulation Experiment

- 1) Enhanced Adaptive Acknowledgement (EAACK) Process will be started.
- 2) The source encrypts data using the destination public key and sends through intermediate nodes.
- 3) After receiving data destination decrypts data using its private key.
- 4) EAACK – Ack process, destination sends ack message to source nodes for the confirmation of data delivery.
- 5) EAACK –SACK (send acknowledgement) process, if sources doesn't receives ack, then S-ACK(Secure Acknowledgment) process begin.
- 6) EAACK-SACK begins for three consecutive neighbor nodes for malicious node detection.
- 7) Third intermediate node 16 sends ack packet to node - 13, but node-13 doesn't sends ack packet.
- 8) Intermediate node-05 sends A(node-16 and node-13 malicious) to source node.

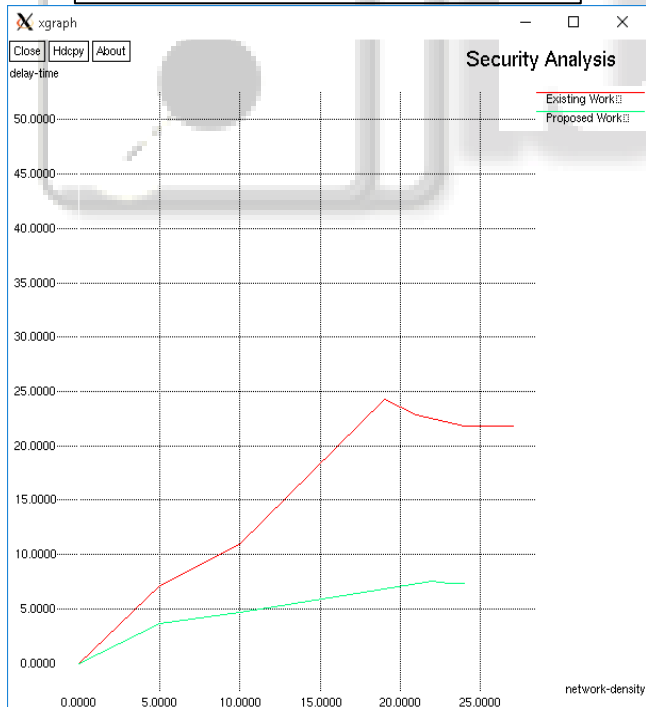
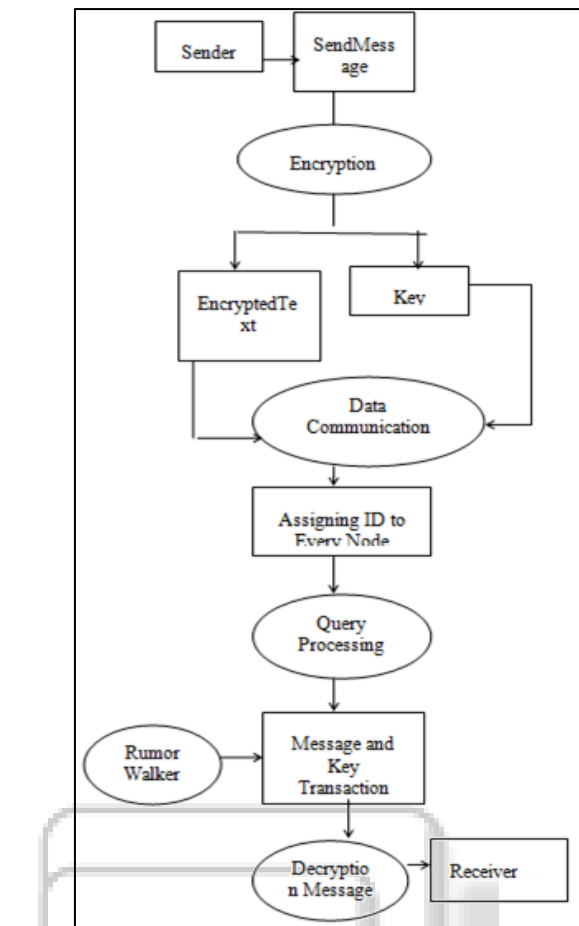


Fig. 1: Throughput of the Proposed System

Shows that the throughput of the proposed system in a pictorial representation. In the planned scheme, not only the attendant verifies the users, but the abuser can also verify the server. Since of the inflexibility of inverting the hash utility $f(.)$, it is computationally infeasible for the attacker to determine (α_i, β_i) , and consequently it is infeasible for him to falsify a cross. If the attacker needs to subterfuge as the AS, he needs to calculate $h = H(K_s, X, Y)$.

He requires xB in order to calculate X . However, xB is the personal key of AS to which the aggressor has no entrance.

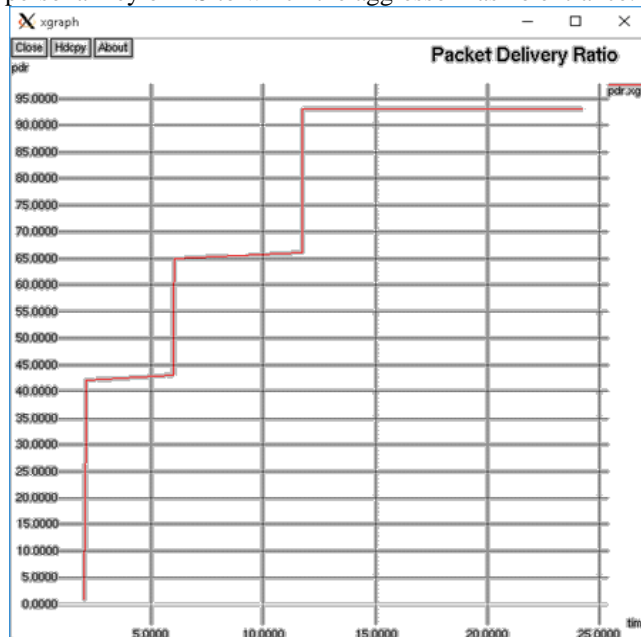


Fig. 2: Packet Delivery Ratio in WSN

Shows that the packet drop rate ratio with each node in the network. The impact of the safekeeping protocol for key production and revocation on packet drop rate in real-time submission is also studied in the simulation. For this purpose, a VoIP submission is invoked between two MRs which produce UDP traffic in the wireless link. The packet drop rates in wireless link when the connection is secluded with the proposed security protocol and when the link is secluded with a static key.

V. CONCLUSION AND FUTURE WORK

Nevertheless, the be existent anonymity proposed techniques are usually introduced as mostly path based. Before transmission, peers select the specific core nodes then assemble paths. The assemble paths remains particularly high by updating and sustaining. The research is carried out to propose mutual anonymity non path based protocol to employ for structure wireless sensor networks. RR issues key and cipher rumors, Rumor riding using random walk to disjointedly and guessing they would be meet in various random peers. RR expanded the higher status of anonymity and efficient performance in particular traffic approach in consequences of identity driven simulation and RR can defend successfully against most popular attacks. We already discussed significant features in security analysis portion that practically implement our prototype. Our speed query ongoing work in traffic produce confuses to attacker and moreover we can reduce the overhead traffic. An information leakage, unlink ability and disaster tolerance, different attacks and these characteristics we examine and analysis by employing the RR security.

A simple mode to get a user's password is to watch them during authentication. This is called shoulder surfing. No substance if keystroke dynamics are used in the verification or identification mode, shoulder surfing is no threat for the authentication system. Password is not used in the identification case and hence the password cannot be stolen. Only the keystroke pattern is substantial and

decisive. In case of verification, an attacker may be able to get the password by shoulder surfing. However, keystroke dynamics for verification is a two-factor authentication mechanism. The keystroke pattern motionless has to match with the stored profile.

REFERENCES

- [1] X. F. Ding and C. G. Ma, "The Three-Party Password-authenticated Key Exchange Protocol with Stronger Security," *Chinese Journal of Computers*, vol. 33, 2010, pp. 111-118, doi: CNKI: SUN: JSJX.0.2010- 01-013.
- [2] O. K. Jeong, I. R. Jeong, K. Sakurai, and D. H. Lee, "Efficient verifier-based password-authenticated key exchange in the three-party setting," *Computer Standards & Interfaces*, vol. 29, 2007, pp. 513- 520, doi: 10.1016/j.csi.2006.12.002.
- [3] D. G. Feng and J. Xu, "A New Client-to-Client Password- Authenticated Key Agreement Protocol," *Computer Science*, vol. 5557, 2009, pp. 63-76, doi: 10.1007/978-3-642-01877-0_7.
- [4] J. W. Byun, I. R. Jeong, D. H. Lee, and C. S. Park, "Password authenticated key exchange between clients with different passwords," *Proc. ICICS 2002*, 2002, pp. 134-136, doi:10.1007/3- 540-36159-6_12.
- [5] J. Y. Kim, S.J. Kim, J. Kwak and D. H. Won, "Cryptanalysis and improvement of password authenticated key exchange between clients with different passwords," *Computational Science and its Applications-ICCSA 2004*, *Lecture Notes in Computer Science*, vol. 3043, pp. 895-902, doi: 10.1007/978-3-540-24707-4_102.
- [6] E.J. Yoon and K. Y. Yoo, "A secure password-authenticated key exchange between clients with different passwords," *Advanced web and network technologies and applications*, *Lecture Notes in Computer Science*, vol. 3842, pp. 659-663, doi: 10.1007/11610496_88.
- [7] X. M. Lui, F. C. Zhou, and G. R. Chang, "A verifier-Based Key Exchange Protocol in Cross-Realm Setting," *Proc. the 2009 International Conference on Networks Security, Wireless Communications and Trusted Computing*, April 2009, pp. 350-353, doi: 10.1109/NSWCTC.2009.304.
- [8] J. W. Byun, D. H. Lee, and J. I. Lim, "EC2C-PAKA: An efficient client-to-client password-authenticated key agreement," *Information Sciences*, vol. 177, 2007, pp. 3995-4013, doi:10.1016/j.ins.2007.03.024.
- [9] X. F. Ding and C. G. Ma, "Cryptanalysis and Improvements of Cross-Realm C2C-PAKE Protocol," *Proc. WASE International Conference on Information Engineering*, July 2009, Taiyuan, China, pp:193-196, doi:10.1109/ICIE.2009.39.
- [10] K. Yoneyama, "Cross-Realm Password-Based Server Aided Key Exchange," *Information Security Application*, vol. 6513, 2011, pp. 322-336, doi: 10.1007/978-3-642-17955-6_24.
- [11] W. Jin and J. Xu, "An Efficient and Provably Secure Cross-Realm Client-to-Client Password-Authenticated Key Agreement Protocol with Smart Cards," *Proc. CANS 2009*, pp. 299-314, doi: 10.1007/978- 3-642-10433-6_20.
- [12] D. Goldschlag, M. Reed, and P. Syverson, "Onion routing", *Communications of the ACM*, 1999.
- [13] A. Medina, A. Lakhina, I. Matta, and J. Byers, "BRITE: an approach to universal topology generation", In *Proceedings of the International Workshop on Modeling, Analysis and Simulation of Computer and Telecommunications Systems (MASCOTS)*, 2001.
- [14] V. Scarlata, B. N. Levine, and C. Shields, "Responder anonymity and anonymous Peer-to-Peer file sharing", In *Proceedings of IEEE ICNP*, 2001