HYBRID CRYPTOGRAPHIC ENHANCEMENT: AN UPDATE TO NETWORK SECURITY

Dr. A. Udhayakumar
Assistant Professor, Department of Computer Science
A.M.JAIN College, Chennai, India
umaudhaya83@gmail.com

ABSTRACT

A network is any set of computing nodes which has the flexibility of exchanging information by interacting with each other meaningfully, permitting resource sharing in a very correct manner. The gathering of computers is interconnected by communication channels, which require to be secure for higher information exchange. This field of networking consists of specialist space of network security adopted by network administrator to stop and monitor unauthorized access, modification and denial of network [12]. To combat the growing drawback, security professionals square measure in search of better protection. Security Attacks compromises the protection and therefore varied even and uneven cryptologic algorithms are projected to realize the protection service in the correct manner, like Authentication, Confidentiality, Integrity, Non-Repudiation and handiness. These algorithms are needed to supply information security and users credibleness. To improve the strength of those security algorithms, a new security algorithmic program is designed exploitation combination of each symmetric and uneven cryptologic techniques [10]. This algorithm provides 3 cryptologic primitives like integrity, confidentiality and authentication. This will be achieved by the combinatorial impact of Threshold Cryptography enforced and Address-based Cryptography Scheme.

Keywords: Authentication, Threshold Cryptography enforced, Address-based Cryptography Scheme

1. Introduction

In Wireless Sensor Networks (WSNs), sensor nodes square measure autonomous and distributed that square measure meant to observe and monitor the phenomena and communicate the same to sink node. Secure knowledge transmission may be a challenge in such Networks. Thanks to the restricted memory resources and energy a constraints, complicated serious key security mechanisms may not be appropriate for resource strained WSNs. Key management in wireless detector network may be a complicated task due to its nature of its constraints. During this paper, a threshold cryptography based mostly key management mechanism is planned. The planned theme considers hierarchal detector network. The Sink node shares the key cluster key to the whole detector node within the network. Threshold cryptography protects the shared key by malicious or interloper node within the network. Proposed technique analysis of defensive threats is proposed. An Address-based Cryptography theme (ACS) is a combination of ad hoc node address and public key cryptography. ACS may be a certificate less public key cryptography solution in that public keys of mobile nodes are directly derivable from their known Ad hoc node address plus some common information. Thus, it eliminates the requirement for certificate-based documented public-key distribution essential in standard Public-key management schemes. ACS is associate economical construction methodology of address-based public/private keys cryptography that not solely ensures high-level authentication to node exchange info, but also enables economical network-wide secure key update via a single broadcast message. It conjointly provides general information regarding a way to select the key sharing parameters used with public key cryptography to satisfy desirable levels of security and authentication. The advantages of ACS over existing certificate-based solutions are even through intensive simulations. The planned theme ACS offers a replacement innovation towards simpler and economical security style.

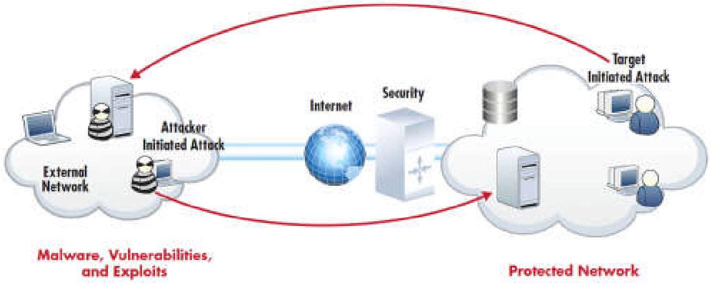

Fig.1 – Network Security: Protected and Unprotected Network

2. Previous Work

In previous couple of year’s advances in electronics devices, small microchip and wireless communication technology made to evolve Wireless device networks (WSN). WSNs have few hundred to thousands of sensors. These sensor nodes are liable for sensing the info from the environment and causation the detected information to the bottom station through intermediate device nodes.WSN’s are getting additional well-liked and quick computing in real time sensing for numerous applications, and plays a vital role within the future network technologies. Achieving QOS for various applications is extremely necessary and gains overall network performance [1]. Since the WSN are deployed in open setting, the attacks and malicious activities are increased. Securing the info and communication between the trustworthy authorities during a secured manner may be a difficult problems within the WSN [2]. A security is a major issue in WSN because it is hospitable nature and unsecured [3]. Many approaches are projected for secure communication to realize security goals for providing information confidential and integrity. Device nodes that collects information periodically, transmits the collected data to Bachelor of Science during a single or multihop transmission. In standard key management techniques could either need trustworthy certificate server or not [1]. The infrastructure less nature of MANETs prevents the utilization of server primarily based protocols like Kerberos [2]. Therefore during this paper specialize in discussing server less and certificate less approaches. All the nodes are preload with a worldwide interchangeable key, which is vulnerable to any purpose of compromise: If any single node is compromised, the safety of the whole network is folded. It lacks quantifiability as a result of it's difficult to ascertain interchangeable keys between existing nodes and new joined nodes. Second, securely updating the general interchangeable keys within the network may be a nontrivial. Last, it needs every node to store (N-1) keys (assume N nodes), which can represent a significant storage overhead during a giant network. Symmetric-key techniques [3] also are given a commonly disadvantage for not supporting economical authentication as a result of every secret's renowned to a minimum of two nodes. There has been heaps of literature on public-key management, these schemes all rely upon certificate based cryptography (CBC), that uses public-key certificates to manifest public keys by binding public keys to the node ID. A main concern with CBC based approaches is that the want for certificate-based public-key distribution. One naive methodology is to preload every node with all the others public-key certificates before network preparation.

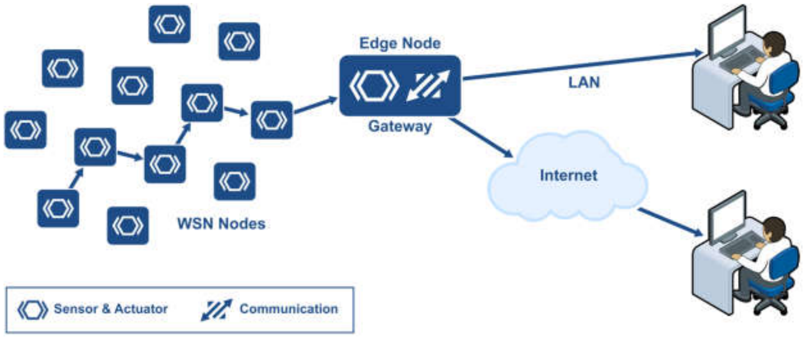

Fig.2 – WSN: Wireless Sensor Network

This approach will neither scale well with the increasing network size, nor handle key update during a secure and cost-effective manner. Another approach of on-demand certificate retrieval ARAN [9] could cause each unfavorable communication latency and infrequently tremendous communication overhead. An economical various to blood profile, ID-based cryptography (IBC) [10] [12] has been gaining momentum in recent years. It permits public keys to be derived from entities renowned identity data, thus eliminating the necessity for public key distribution and certificates. This nice feature has galvanized a couple of IBC based certificate less public-key management In this paper, it finds the new answer for existing public key management; it's Associate in Nursing address primarily based cryptography key management theme, called ACS.

3. Threshold Cryptosystem

In cryptography, a cryptosystem is called a threshold cryptosystem, if in order to decrypt an encrypted message or to sign a message, several parties (more than some threshold number) must cooperate in the decryption or signature protocol.

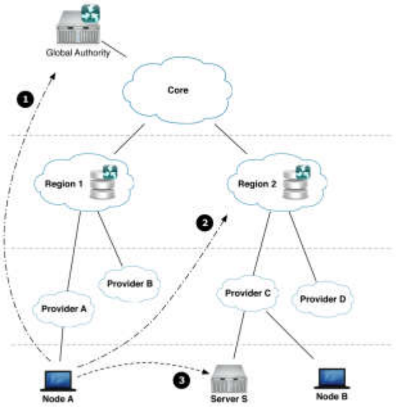

Fig.3 – Working Procedure

The message is encrypted using a public key and the corresponding private key is shared among the participating parties. Let n be the number of parties. Such a system is called (t,n) - threshold, if at least t of these parties can efficiently decrypt the ciphertext, while less than t have no useful information. Similarly it is possible to define (t,n)-threshold signature scheme, where at least t parties are required for creating a signature. Perhaps the first system with complete threshold properties for a trapdoor function (RSA).

4. ACS: Address-based Cryptography Scheme

Uses the node address with certificate less cryptography to give the top to finish authentication. Route invention in ACS relies on route invention packet from supply node and route reply packet from destination node. The route packets area unit encrypted supported ACS. Only authorized nodes participate at every hop between source and therefore the destination. Assume key generation is known by all licensed nodes.

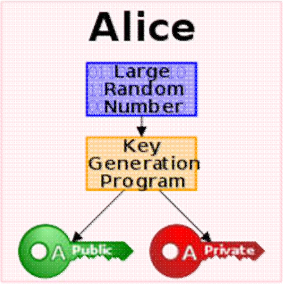

Fig.4 – Working Procedure

5. System Architecture

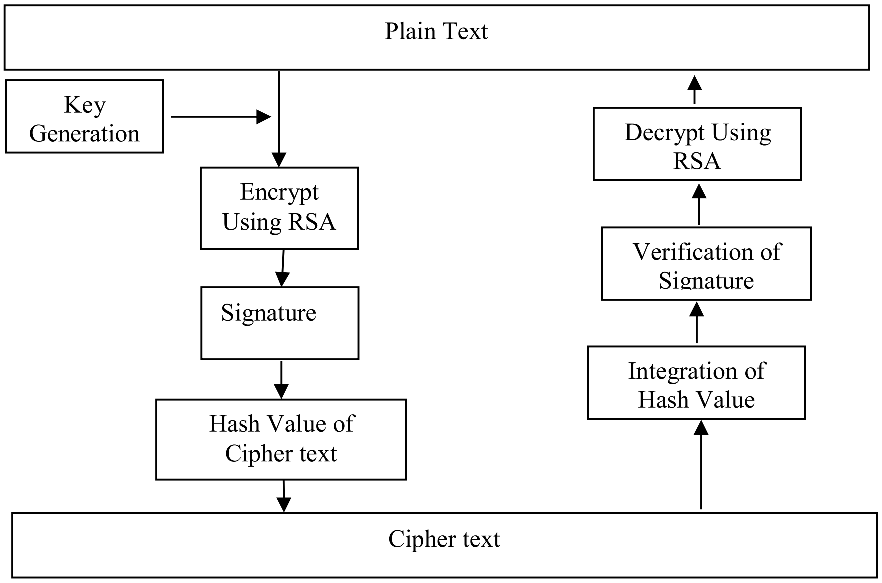

Fig.3 –Architecture Diagram

References

[1] Darrel Hankerson, Julio Lopez Hernandez, Alfred Menezes, Software Implementation of Elliptic Curve Cryptography over Binary Fields, 2000, Available at http://citeseer.ist.psu.edu/hankerson00software.html

[2] Certicom, Standards for Efficient Cryptography, SEC 2: Recommended Elliptic Curve Domain Parameters, Version 1.0, September 2000, Available at http://www.secg.org/download/aid-386/sec2_final.pdf

[3] E. Jochemsz and A. May, “A polynomial time attack on standard RSA with private CRT-exponents”, 2007.

[4] M. J. Hinek, “Another look at small RSA exponents,” in Topics in Cryptology-CT-RSA 2006, ser. Lecture Notes in Computer Science, D. Pointcheval, Ed. New York: Springer, 2006, vol. 3860, pp. 82–98.

[5] Ravindra Kumar Chahar and et.al., “ Design of a new Security Protocol”, IEEE International Conference on Computational Intelligence and Multimedia Applications, pp 132 – 134, 2007. [6] Ekta, Ranjeet Kaur Light “Fidelity (LI-FI)-A Comprehensive Study” International Journal of Computer Science and Mobile Computing Vol. 3, Issue. 4, April 2014, pg.475 – 481 ISSN 2320–088X

[6] Akyildiz, Ian F., Weilian Su, Yogesh Sankarasubramaniam, and Erdal Cayirci. "Wireless sensor networks: a survey." Computer networks 38, no. 4 (2002): 393-422.

[7] Papalexakis, Evangelos E., Alex Beutel, and Peter Steenkiste. "Network anomaly detection using co-clustering." In Encyclopedia of Social Network Analysis and Mining, pp. 1054-1068. Springer New York, 2014.

[8] Zhou, Lidong, and Zygmunt J. Haas. "Securing ad hoc networks." IEEE network 13, no. 6 (1999): 24-30.

[9] Cai, Zhipeng, Shouling Ji, Jing He, and Anu G. Bourgeois. "Optimal distributed data collection for asynchronous cognitive radio networks." In Distributed Computing Systems (ICDCS), 2012 IEEE 32nd International Conference On, pp. 245-254. IEEE, 2012.

[10] Ji, Shouling, and Zhipeng Cai. "Distributed data collection and its capacity in asynchronous wireless sensor networks." In INFOCOM, 2012 Proceedings IEEE, pp. 2113-2121. IEEE, 2012.

[11] Ji, Shouling, Raheem Beyah, and Zhipeng Cai. "Snapshot/continuous data collection capacity for large-scale probabilistic wireless sensor networks." In INFOCOM, 2012 Proceedings IEEE, pp. 1035-1043. IEEE, 2012.

[12] Ji, Shouling, Raheem Beyah, and Zhipeng Cai. "Snapshot/continuous data collection capacity for large-scale probabilistic wireless sensor networks." In INFOCOM, 2012 Proceedings IEEE, pp. 1035-1043. IEEE, 2012.

[13] Buttyán, Levente, and Jean-Pierre Hubaux. "Stimulating cooperation in self-organizing mobile ad hoc networks." Mobile Networks and Applications 8, no. 5 (2003): 579-592..

[14] Zhang, Yanchao, Wenjing Lou, Wei Liu, and Yuguang Fang. "A secure incentive protocol for mobile ad hoc networks." Wireless Networks 13, no. 5 (2007): 569-582.

[15] Weyland, Attila, and T. Braun. "Cooperation and accounting in multihop cellular networks." PhD diss., PhD thesis, Univ. of Bern, 2005.

[16] Weyland, Attila, Thomas Staub, and Torsten Braun. "Comparison of motivation-based cooperation mechanisms for hybrid wireless networks." Computer communications 29, no. 13 (2006): 2661-2670.

[17] Zhong, Sheng, Jiang Chen, and Yang Richard Yang. "Sprite: A simple, cheat-proof, credit-based system for mobile ad-hoc networks." In INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies, vol. 3, pp. 1987-1997. IEEE, 2003.

[18] P. Papadimitratos and Z. J. Haas, “Secure routing for mobile ad hoc networks,” in Proc. SCS CNDS, San Antonio, TX, Jan. 27– 31, 2002, pp. 193–204.

[19] B. Newman and T. Tso, “Kerberos: An Authentication Service for Computer Networks,” IEEE network Mag., vol. 32, no. 9, pp. 33-38, Sept. 1994.

[20] Y. Hu, A. Perrig, and D. B. Johnson, “Secure efficient distance vector routing for mobile wireless ad hoc networks,” Elsevier Ad Hoc Networks, vol. 1, no. 1, pp. 175–190, Jul. 2003.

[21] L. Zhou and Z. J. Haas, “Securing Ad Hoc Networks,” IEEE Networks, vol. 13, no. 6, pp. 24-30, 1999.

[22] J. Kong, P. Zerfos, H. Luo, S. Lu, and L. Zhang, “Providing Robust and Ubiquitous Security Support for Mobile Ad Hoc Networks,” Proc. IEEE Int’l Conf. Network Protocols, Nov. 2001.

[23] M. Narasimha, G. Tsudik, and J.H. Yi, “On the Unitility of Distributed Cryptography in P2P and Manets: The Case of Membership Control,” Proc. IEEE Int’l Conf. Network Protocols, Nov. 2003.

[24] S. Yi and R. Kravets, “Moca: Mobile Certificate Authority for Wireless Ad Hoc Networks,” Proc. Second Ann. PKI Research Workshop (PKI ’03), Apr. 2003.

[25] M. Bechler, H.-J. Hof, D. Kraft, F. Pahlke, and L. Wolf, “A Cluster- Based Security Architecture for Ad Hoc Networks,” Proc. IEEE INFOCOM, Mar. 2004.

[26] K. Sanzgiri, D. LaFlamme, B. Dahill, B. Levine, C. Shields, and E.Belding-Royer, “Authenticated Routing for Ad Hoc Networks,” IEEE J. Selected Areas Comm., voaszxxl. 23, no. 3, pp. 598-610, Mar. 2005.

[27] A. Shamir, “Identity Based Cryptosystems and Signature Schemes,” Proc. CRYPTO’84, pp. 47-53, 1984.

[28] A. Khalili, J. Katz, and W. Arbaugh, “Toward Secure Key Distribution in Truly Ad Hoc Networks,” Proc. IEEE Workshop Security and Assurance in Ad Hoc Networks, Jan. 2003.

Dr A.Udhayakumar Msc., MCA., M.Phil., Ph.D., NET., SET., received his B.Sc., and M.Sc., degree in Computer Science from the Bharathidasan University in 2003 and 2005 respectively. He received his M.Phil degree in Computer Science from Alagappa University in the year 2009. He was awarded his Ph.D., degeree from Karpagam University, Tamilnadu India focusing on "Multi-party Mobile Computing security". He joined as an Assistant Professor in the Department of Computer Science A.M.JAIN College, Meenambakkam, Chennai-114 affiliated to the University of Madras Tamilnadu , India in the year 2005.He has 12 years Teaching Experience in Computer Science Department. He is the author/co-author for more than 15 National papers and 10 International Journal Published. He is the co-author of "Elements of Computer Networks". He is the author of UGC-NET solved papers 2004-2018.His papers have received a wide range of awards in the National seminars and conferences . His area of interest is the field of Network security. He cleared his SET and NET examination 2016 and 2017 respectively.