International Journal of Electronics Engineering (ISSN: 0973-7383)
Volume 11 • Issue 1 pp. 831-838 Jan 2019-June 2019 www.csjournals.com

A Review: Analysis of Various Techniques for Cryptography

Er. Amandeep Singh Bhandari, Dr. Charanjit Singh
Department of ECE, Punjabi University, Patiala, Punjab, India

Abstract: Security is an important issue in information and communication fields as it protects information and data from unauthorized access. In order to provide perfect security, the user and the device connected to data and communication network must be authenticated. The protection of data from threats and attacks can be achieved by cryptography. It provides techniques, mechanisms, and tools for private and authenticated communication, and for performing secure and authenticated transactions over internet. All networked computers and devices must have cryptographic layers implemented, and must be able to access to cryptographic functions in order to provide security features. In this paper, various techniques for cryptography have been reviewed, based on conference key establishment, mutual authentication and session key exchange, session key distribution, and key management.

Keywords: cryptography, conference key establishment, mutual authentication and session key exchange, session key distribution, and key management.

Introduction

In cryptographic terminology, the message is called plaintext. Encoding the contents of the message in such a way that its contents cannot be unveiled by outsiders is called encryption. The encrypted message is called the ciphertext. The process of retrieving the plaintext from the ciphertext is called decryption. Encryption and decryption usually make use of a key and the coding method use this key for both encryption and decryption. Once the plaintext is coded using that key then the decryption can be performed only by knowing the proper key [2].

Different techniques are used for data encryption and decryption based upon key which are as follows:

A. Symmetric Cryptography

If sender and recipient use the same key, it is known as symmetric or private key cryptography. It is always suitable for long data streams. Such system is difficult to use in practice because the sender and receiver must know the key. It also requires sending the keys over a secure channel from sender to recipient.

The main concern behind symmetric encryption is how to share the secret key securely between the two parties. If the key gets known for any reason, there can be threat to leakage of data. The key management for this type of encryption is troublesome when a unique secret key is used for each peer-to-peer connection. The total number of secret keys to be saved and managed for n-nodes will be $n(n-1)/2$.

B. Asymmetric Cryptography

If sender and recipient use different keys, it is known as asymmetric or public key cryptography. The key used for encryption is called the public key and the key used for decryption is called the private key. Such technique is used for short data streams and also requires more time to encrypt the data.
To encrypt a message, a public key can be used by anyone, but the owner having private key can only decrypt it. There is no need for a secure communication channel for the transmission of the encryption key. Asymmetric algorithms cannot be applied to variable-length streams of data. Asymmetric keys are also called a key-exchange pair. Asymmetric encryption techniques are slower than symmetric techniques, because they require more computational processing power.
To get the benefits of both methods, a hybrid technique is usually used. In this technique, asymmetric encryption is used to exchange the secret key; symmetric encryption is then used to transfer data between sender and receiver. It is easy to convert the private key into public key, but the reverse is very difficult.

II. LITERATURE REVIEW

This section involves the work done by the various researchers in the field of cryptographic algorithm for data security in wireless networks.

Cryptography has a long and fascinating history. The most complete non-technical account of the subject is Kahn's "The Code breakers" that include cryptography from its initial and limited use by the Egyptians some 4000 years ago, to the twentieth century where it played a crucial role in the outcome of both world wars (D. Kahn, 1996).

Secured data transmission includes a conference key establishing scheme for mobile communications based upon RSA (Ron Rivest, Adi Shamir, and Leonard Adleman) and congruence mechanism, proposed by Hwang et al (1995), further was improved by Hwang (1999) to allow dynamic joining and leaving from the conference. It was observed insecure against eavesdropping by Ng (2001), which overcomes Hwang's weakness with a small modification in the key establishing procedure between the conference bridge and the new participant. An efficient conference scheme for mobile was also proposed by Yi Xun et al (2003) based on modular square root, which was secure against eavesdropping, impersonating, and tracking attack that allows a participant to join/ leave dynamically. This scheme was found to be insecure against replay attacks; therefore, modified by Zhiguo Wan et al (2006). In addition to security of conferences from various attacks, the conferees were prevented from submitting fraud or invalid messages based on verifiable random number suggested by Liu et al (2009). Some flaws were also observed in the schemes presented by Yi Xun et al (2003) and Z.G Wan et al (2006) and modified by He et al (2012) using improved protocol based on High Level Protocol Specification Language (HLPSL), and verified using the model checking tool Automated Validation of Internet Security Protocols and Applications (AVISPA). Lou et al (2013) provides a scheme which illuminates the need of conference bridge or interactive communication; thus it saved communication overhead.

Another method to protect data transmission includes the Mutual Authentication and Session Key Exchange Protocols (MAKEPs) proposed by Park et al (1997) based on dynamic certificates to protect the session key. Two MAKEPs were proposed by Wong et al (2001), namely server-specific and linear MAKEPs to reduce the computational requirement of interaction between server and client. This scheme was observed insecured against unknown key-share attacks by K. Shim (2003); thus modified using the identities of the sender and intended recipient in the messages being encrypted. Some pitfalls were also observed in this scheme and improved by Ng et al (2004). An authentication technique used for mutual authentication and session key exchange for Global Mobility Network (GLOMONET) was introduced by Suzuki et al (1997). It was observed insecured against various attacks and improved by Buttyan et al (2000). An RSA-based authenticated key exchange protocol was also proposed by Zhu et al (2002) to be implemented on low-power devices by reducing the computational complexity. This protocol was observed insecured against online password guessing attacks by Her-Tyan et al (2003) and also explicit key authentication was not provided. Therefore, the session key confirmation was provided in order to achieve the explicit key authentication and modified the protocol to protect it from attacks. Further, improvement was done by Zhang (2005) to protect the session key from e-residue attack. Hwang et al (2003) introduced a Self-encryption technique for both roaming services and regular communication. This technique was further improved by Long et al (2004) in which the intervention of a roaming user's home network was mitigated for authentication between a visited network and the roaming user. Hwang et al's scheme (2003) was observed insecured against active and passive attacks by (Feng, 2006). Two sets of MAKEPs were proposed by Jiang et al (2006) with anonymity property for roaming service using the secret-splitting principle and self-certified scheme to hide the real identity of the mobile user in roaming network environment. Another efficient authentication protocol with user anonymity was presented by Zhu et al (2004) based on hash functions and smart cards using only symmetric encryption and decryption. Lee et al (2006) modified this protocol further, by removing some weaknesses such as imperfect backward secrecy, no mutual authentication, and risk of forgery attack, and thus the security and efficiency of the protocol was increased significantly. The scheme failed to provide anonymity, and subsequently exposed the identity of a mobile user to foreign agents. Wu et al (2008) improved it by providing protection against off-line guessing attack and achieves anonymity. But Zheng et al (2009) and Lee et al (2009) evaluated that none of schemes presented by Zhu et al (2004) and Wu et al (2008) provided anonymity. Mun et al (2012) also showed few deficiencies in the scheme presented by Wu et al (2008) such as, failed to achieve anonymity and perfect forward secrecy, and disclosing of legitimate user's password. Hence, these deficiencies were improved in their scheme. They also provided mutual authentication and resistance to man-in-the-middle attack. The scheme presented by Zhu et al (2004) was observed to be vulnerable to a replay attack and two impersonation attacks. Among these vulnerabilities, this scheme was insecured against the impersonation attack with smart card security breach. So, He et al (2011) proposed a secure and light-weight user authentication scheme in which mutual authentication with user anonymity was achieved and protected the key from various attacks. Li et al (2012) observed that the scheme was vulnerable to eavesdropping attacks; therefore, treated as insecured and could not be used for real time applications. So, an enhanced version of user authentication scheme was presented to provide user anonymity. It was also identified that the scheme introduced by He et al (2011) failed to achieve strong two-factor security, and also suffered from domino effect, privileged insider attack and no password change option, etc. An enhanced authentication scheme with privacy preservation based on quadratic residue assumption was proposed by Jiang et al (2013) to achieve two-factor security and user untraceability. This scheme was critically analyzed and showed that it was insecured against stolen-verifier attack and replay attack. So, a new protocol was proposed by Wen et al (2013) which did not require the home agent to share a static secret key with the foreign agent, and hence, it was more practical and realistic. The scheme presented by Mun et al (2012) was carefully analyzed and showed that it was vulnerable to impersonation attacks, off-line password guessing attacks and insider attacks, and did not provide user friendliness, user's anonymity, proper mutual authentication and local verification. So, a novel anonymous authentication scheme was proposed by Zhao et al (2014) for roaming service in global mobility networks using elliptic curve cryptosystem to not only protect the scheme from security breaches, but also emphasized the efficient features. It was reported that the robust secure and effective anonymous authentication scheme proposed in this scheme was suffered from offline password guessing attacks, impersonation attacks and privileged insider attacks. So, an efficient and secured anonymous communication for location based service using asymmetric cryptography scheme was proposed by Memon et al (2015) to prevent such attacks and provide mutual authentication to make the system more secured.

Another method to protect data transmission includes the periodic distribution of a session key to group members in secured multicast communication. More research was done for key distribution over reliable channels, but a self-healing key distribution scheme with revocation capability was presented by Staddon et al (2002) to retrieve lost group keys on their own, without requesting additional transmissions from the group manager, thus mitigating network traffic as well as load on group manager. This scheme was enhanced by Liu et al (2003) to be used in highly mobile, volatile and hostile wireless networks. The communication overhead and the storage overhead were also reduced to prolong the lifetime of wireless devices. The scheme presented by Staddon et al (2002) was analyzed and modified by Blundo et al (2004) in order to reduce the communication complexity and memory storage further than evaluated by Liu et al (2003). In the modified scheme, the user was able to recover all keys associated with sessions from one broadcast message. It was also observed that the previous schemes did not hold lower bound on the size of the broadcast message. So, a new definition of self-healing key distribution was proposed by Blundo et al (2006) in which the scheme presented by Staddon et al (2002) was modified and extended in order to provide some lower bounds on the resources required for implementing such schemes. Some deficiencies in previous schemes were improved by the scheme presented by Dutta et al (2007) in which the personal key was reused to next m sessions without any alteration and the maximum session number (m) was no longer needed to be determined in setupphase. This scheme was further improved by Dutta et al (2008) by reducing communication overhead without increasing storage cost. It was evaluated that the schemes presented by Dutta et al (2007, 2008) were insecured against random attacks (Daza et al, 2009). A new self-healing key distribution scheme with sponsorization capability for infrastructure-less wireless networks was proposed by Han et al (2009) in which the length of broadcast message was shortened to reduce storage overhead. Wang et al, 2011 observed some flaws in this scheme that it was not capable to provide forward and backward security as some internal users generated a new session key. This scheme was resulted as insecured to be implemented in wireless networks. A new mechanism was presented by Rams et al (2013) to achieve backward secrecy in long-lived self-healing group key distribution schemes based on exponential arithmetic. The security analysis of the scheme proved that the forward and backward secrecy was achieved, and also collusion between the newly joined users and the revoked ones was avoided. Two improved Self-healing Group Key Distribution (SGKD) schemes using the One-way Hash Chain (OHC) and Revocation Polynomial (RP) in resource-constrained wireless networks were proposed by Chen et al (2014) in which some novel methods were presented to utilize one-way hash chain, and to construct the personal secret, the revocation polynomial and the key updating broadcast packet. By this, the collusion attack resistance problem in existing HC-SGKD schemes was solved. Simulation results proved that the proposed OHC and RP-SGKD schemes were practical for resource constrained wireless networks in bad environments where a strong collusion attack resistance was required and many users should be revoked. This scheme was analyzed to be insecured due to presence of some security flaws found by Zheng et al (2014) in which a revoked user recovered other legitimate user's personal secrets which could be used to recover the current session's session key, this directly broke the forward security, revocation capability and collusion attack resistance capability.

For secured communication, it is necessary to use appropriate cryptographic algorithms to provide the required security services. The efficient algorithms require correct protocols for authentication and key management. A variety of protocols specifically designed for use in mobile applications were proposed by many authors (A. Aziz et al, 1994; Basyouni et al, 1997; Beller et al (1991-93); Park et al, 1994; Varadharajan et al, 1996). A hybrid authenticated key-establishment protocol was proposed by Qiang Huang et al (2003) in which both asymmetric- and symmetric-key cryptographic techniques were used to reduce computation by providing fast processing speed and less communication overhead. This protocol was analyzed by X. Tian et al (2005) and observed that it was insecured against various attacks. Thus, the security of the protocol was enhanced by generating the long-term private key randomly, so that, an attacker could not get the key easily. It was observed that the protocol proposed by Qiang Huang et al (2003) and improved by X. Tian et al (2005) did not provide perfect forward secrecy. In order to address with this problem, an improved protocol was proposed by Yoon et al (2006). This protocol also provided protection against various attacks and less communication overhead. A novel distributed key management scheme based on Exclusion Basis Systems (EBS) was proposed by Younis et al (2006) for management of encryption keys in large-scale clustered networks. This scheme was proved to be highly scalable, hierarchical, efficient, location-aware, and light-weight. A multi-group key management scheme was presented by Yan et al (2007) to achieve forward and backward secrecy based on hierarchical group access control. A probabilistic unbalanced key management scheme LIGER was designed and implemented by Patrick Traynor et al (2007) to provide security in potentially dynamic environments. An efficient key management scheme, namely, Key Tree Reuse (KTR) was proposed by QijunGu et al (2009) to handle key distribution with regard to complex subscription options and user activities. The simulation results proved that this scheme reduces communication overhead and decryption cost significantly. SaberBanihashemian et al (2010) proposed a new key management scheme based on random key pre-distribution in which probability of key sharing and resiliency against node capture was increased. A centralized conference key management mechanism based on the elliptic curve cryptography and Lagrange interpolation was introduced by M. H. Guo et al (2011) which provided forward and backward secrecy, less computing cost, and protection against various attacks. A new approach for generating keys from available data was proposed by Ajay Kakkar et al (2012) to provide a more secure cryptographic model with a minimum number of overheads. A group key management mechanism was proposed by M. H. Guo et al (2012) for data communication in Vehicular Ad hoc Networks (VANETs). This mechanism was developed on the basis of a decentralized architecture with hierarchical key tree and cluster heads. It provides a rekeying method to reduce the communication cost, also better forward and backward security was achieved. A new key management scheme based on two-dimensional backward key chains was presented by Sujuni Li et al (2012) for Multiple Deployment Sensor Networks (MDSNs). The security analysis and simulation results indicated that the scheme provides high local connectivity with a low storage overhead. An efficient hierarchical key management system was presented by Chien-Ming Chen et al (2014) for a heterogeneous cluster based Wireless Sensor Network (WSN). The system utilized symmetric cryptographic algorithms and low cost operations such as bitwise XOR operation and modular multiplication. The simulation results proved that the mechanism was efficient in storage, communication, and computation. An efficient group key management scheme based on Logical Key Hierarchy Plus (LKH++) algorithm was proposed by Wenbin Yao et al (2015) for heterogeneous sensor networks. This scheme provided protection against node compromise attacks by separating key management and key distribution methods to enhance the network security. A slot based multiple group key management scheme was proposed by Trust T. Mapoka et al (2015) to improve the key management performance and authentication during handoff process. Two rekeying approaches, namely, pairwise and Logical Key Hierarchy (LKH) were implemented to significantly reduce communication bandwidth overhead, storage overheads.Jiming Yao et al (2016) proposed a group-based secure authentication and key agreement (GBS-AKA) scheme in which the majority redundant signaling, and lighten the level of congestion in the core network have been reduced. Also the authentication delay distinctly has been reduced and varieties of malware attacks have been prevented. Furthermore, this protocol greatly improved bandwidth consumption and signaling congestion.A hierarchical group based mutual authentication scheme, HGMAKA has been proposed by ProbiditaRoychoudhury et al (2017) for Machine Type Communication over LTE network. This protocol has reduced the overall signalling load on the access network eNBs. Muzammil M. Ahmad and Sibghatullah I. Khan (2017) provided a three-tier authentication system having three servers, two intermediate servers and an application server to check the authenticity of the client at three independent channels. The application server is used to concatenate the messages received from intermediate servers and compare it with the message received from the client, thereby authenticating the client and servers through same session key. A user authentication scheme based onimproved challenge-response mechanism has been presented by Yuxiang Feng et al (2017) to avoid replay attack and an efficient mutual user authentication and a secure session key agreement have been achieved.A dynamic group based efficient and secure (DGBES-AKA) protocol has been proposed by Shubham Gupta et al (2017) to achieve mutual authentication between MTC devices and core network thereby provided data integrity, confidentiality and key secrecy in terms of KFS/KBS for large number of MTCDs. This protocol has reduced the signalling congestion to large extent and also avoided many vulnerable attacks. Prasanta Kumar Roy et al (2017) proposed a new enhanced two-factor authentication scheme to provide mutual authentication between the communicating parties and to establish a proper session key between them.The protocol was implemented using HLPSL language and formally validated using AVISPA tool to ensure its ability to withstand several attacks.A highly secured 2-way authentication protocol has been proposed by Binu P K et al (2018) to provide mutual authentication between client and server using Zero Knowledge Protocol (ZKP) for web applications ensuring data confidentiality and integrity. ZKP has been implemented with the help of Diffie-Hellman key exchange algorithm to verify the authenticity of the user for the access of services provided by the portal. Balu L. Parneet al (2018) analysed the GBS-AKA protocol proposed by Jiming Yao et al (2016) and found it failed to provide full security to MTCDs and also not able to avoid impersonation and DoS attacks, thereby failed to maintain KFS/KBS. To rectify these problems, a security enhanced group based (SEGB-AKA) protocol has been proposed by solving the problem of the single key during the authentication process.

III. CONCLUSION:

Various authentication techniques for cryptography in terms of mutual authentication, session key exchange, and key management are analysed based on many parameters like disclosure of user identity,computational complexity, forward/backward secrecy, shared key protection, etc. At first, work done by numerous authors was reviewed and then compared based on aforesaid parameters. Many of threats and attacks such as replay attack, redirection attack, DDoS attack, man-in-the-middle attack, etc. to LTE network have been discussed. Also a number of protocols such as DGBES-AKA, GBS-AKA,SEGB-AKA etc. are used to remove such attacks.Aong all protocols, DGBES-AKA and SEGB-AKA provided better KFS/KBS. Some of the protocols used dynamic policies to provide complete authentication, integrity, confidentiality, better key management and forward/backwardsecrecy for LTE networks.

References:

[1] Keromytis, Angelos D., Jason L. Wright, and Theo De Raadt, “The Design of the {OpenBSD} Cryptographic Framework”, In USENIX Annual Technical Conference, General Track, 2003, pp. 181-196.

[2] W. Diffie and M. Hellman, “New Directions in Cryptography”, IEEE Transaction on Information Theory, Vol. IT-22**,** 1976, pp. 644-654**.**

[3] William Stallings, “Cryptography and Network Security: Principles and Practice, Pearson Publications, 2011

[4] Richard E. Blahut, “Cryptography and Secure Communication”, Cambridge University Press, 2014.

[5] Randall K. Nichols, Panos C. Lekkas, “Wireless Security: Models, Threats, and Solutions”, McGraw-Hill, 2002.

[6] D. Forsberg, G. Horn, W. Moeller, V. Niemi, “LTE Security”, John Wiley & Sons, Ltd., Publication, 2013.

[7] D. Kahn, “The Codebreakers: The Story of Secret Writing”, MacMillan publishing, 1996.

[8] M. S. Hwang and W. P. Yang, “Conference Key Distribution Protocols for Digital Mobile Communication Systems”, IEEE Journal on Selected Areas in Communications, 1995, Vol. No. 13, Issue No. 2, pp 416- 420.

[9] M. S. Hwang. “Dynamic Participation in a Secure Conference Scheme for Mobile Communications”, IEEE Transactions on Vehicular Technology, 1999, Vol. No. 48, Issue No. 5, pp 1469 - 1471.

[10] S. L. Ng, “Comments on ‘Dynamic Participation in a Secure Conference Scheme for Mobile Communications”, IEEE Transactions on Vehicular Technology, 2001, Vol. No. 50 pp.334-335.

[11] Yi Xun, Siew Chee Kheong, Tan Chik How, “A Secure and Efficient Conference Scheme for Mobile Communications”, IEEE Transactions on Vehicular Technology, 2003, Vol. No. 52, Issue No. 4, pp 784- 793.

[12] Z.G Wan, Feng Bao, R. H. Deng., “Security Analysis on a Conference Scheme for Mobile Communications”, IEEE Transaction on Wireless Communication, 2006, Vol. No. 5, Issue No. 6, pp.1238-1240.

[13] Liu, Yining, Jianyu Cao, and Min Zeng, “Mobile Conference Scheme Based on Verifiable Random Number”, Second International Symposium on Information Science and Engineering, IEEE, 2009, pp. 177-180.

[14] He, Daojing, Chun Chen, Maode Ma, and Jiajun Bu, “Cryptanalysis of Some Conference Schemes for Mobile Communications”, Security and Communication Networks, 2012, Vol. No. 5, Issue No. 1, pp 107-112.

[15] Lou, Der-Chyuan, Kuo-Ching Liu, and Hui-Feng Huang, “Efficient Mobile Conference Scheme for Wireless Communication”, Informatica, 2013, Vol. No. 24, Issue No. 1, pp 59-70.

[16] Park, Chang-Seop, “On Certificate-Based Security Protocols for Wireless Mobile Communication Systems”, Network, IEEE, 1997, Vol. No. 11, Issue No. 5, pp 50-55.

[17] Wong, Duncan S., and Agnes H. Chan, “Mutual Authentication and Key Exchange for Low Power Wireless Communications”, In Military Communications Conference and Communications for Network-Centric Operations: Creating the Information Force. IEEE, 2001, Vol. No. 1, pp. 39-43.

[18] Shim, Kyungah, “Cryptanalysis of Mutual Authentication and Key Exchange for Low Power Wireless Communications”, Communications Letters, IEEE, 2003, Vol. No. 7, Issue No. 5, pp 248-250.

[19] Ng, Siaw-Lynn, and Chris Mitchell, “Comments on Mutual Authentication and Key Exchange Protocols for Low Power Wireless Communications”, IEEE Communications Letters, 2004, Vol. No. 8, Issue No. 4, pp 262-263.

[20] Suzuki, Shigefusa, and Kazuhiko Nakada, “An Authentication Technique Based on Distributed Security Management for the Global Mobility Network”, Selected Areas in Communications, IEEE Journal, 1997, Vol. No. 15, Issue No. 8, pp 1608-1617.
[21] Buttyan, Levente, Constant Gbaguidi, Sebastian Staamann, and Uwe Wilhelm, “Extensions to an Authentication Technique Proposed for the Global Mobility Network”, IEEE Transactions on Communications, 2000, Vol. No. 48, Issue No. 3, pp 373-376.
[22] Zhu, Feng, Duncan S. Wong, Agnes H. Chan, and Robbie Ye, “Password Authenticated Key Exchange Based on RSA for Imbalanced Wireless Networks”, In Information Security, Springer Berlin Heidelberg, 2002, pp. 150-161.
[23] Her-Tyan, Yeh, Sun Hung-Min, Yang Cheng-Ta, Cheng Bing-Cheng, and Shin-Mu Tseng, “Improvement of Password Authenticated Key Exchange Based on RSA for Imbalanced Wireless Networks”, IEICE Transactions on Communications, 2003, Vol. No. 86, Issue No. 11, pp 3278-3282.
[24] Zhang, Muxiang, “Breaking an Improved Password Authenticated Key Exchange Protocol for Imbalanced Wireless Networks”, IEEE Communications Letters, 2005, Vol. No. 9, Issue No. 3, pp 276-278.
[25] Hwang, Kuo-Feng, and Chin-Chen Chang, “A Self-Encryption Mechanism for Authentication of Roaming and Teleconference Services”, IEEE Transactions on Wireless Communications, 2003, Vol. No. 2, Issue No. 2, pp 400-407.
[26] Long, M., C-H. Wu, and J. D. Irwin, “Localised Authentication for Inter-Network Roaming Across Wireless LANs”, IEEE Proceedings-Communications, 2004, Vol. No. 151, Issue No. 5, pp 496-500.
[27] Bao, Feng, “Analysis of a Secure Conference Scheme for Mobile Communication”, IEEE Transactions on Wireless Communications, 2006, Vol. No. 5, Issue No. 8, pp 1984-1986.
[28] Jiang, Yixin, Chuang Lin, XueminShen, and Minghui Shi, “Mutual Authentication and Key Exchange Protocols for Roaming Services in Wireless Mobile Networks”, IEEE Transactions on Wireless Communications, 2006, Vol. No. 5, Issue No. 9, pp 2569-2577.
[29] Zhu, Jianming, and Jianfeng Ma, “A New Authentication Scheme with Anonymity for Wireless Environments”, IEEE Transactions on Consumer Electronics, 2004, Vol. No. 50, Issue No. 1, pp 231-235.
[30] Lee, Cheng-Chi, Min-Shiang Hwang, and I-En Liao, “Security Enhancement on a New Authentication Scheme with Anonymity for Wireless Environments”, IEEE Transactions on Industrial Electronics, 2006 Vol. No. 53, Issue No. 5, pp 1683-1687.
[31] Wu, Chia-Chun, Wei-Bin Lee, and Woei-JiunnTsaur, “A Secure Authentication Scheme with Anonymity for Wireless Communications”, IEEE Communications Letters, 2008, Vol. No. 12, Issue No. 10, pp 722-723.
[32] Zeng, Peng, Zhenfu Cao, Kim-Kwang Raymond Choo, and Shengbao Wang, “On the Anonymity of Some Authentication Schemes for Wireless Communications”, IEEE Communications Letters, 2009, Vol. No. 13, Issue No. 3, pp 170-171.
[33] Lee, Ji-Seon, Jik Hyun Chang, and Dong Hoon Lee, “Security Flaw of Authentication Scheme with Anonymity for Wireless Communications”, IEEE Communications Letters, 2009, Vol. No. 13, Issue No. 5, pp 292-293.
[34] Mun, Hyeran, Kyusuk Han, Yan Sun Lee, Chan YeobYeun, and Hyo Hyun Choi, “Enhanced Secure Anonymous Authentication Scheme for Roaming Service in Global Mobility Networks”, Mathematical and Computer Modelling, 2012, Vol. No. 55, Issue No. 1, pp 214-222.
[35] He, Daojing, Maode Ma, Yan Zhang, Chun Chen, and Jiajun Bu, “A Strong User Authentication Scheme with Smart Cards for Wireless Communications”, Computer Communications, 2011, Vol. No. 34, Issue No. 3, pp 367-374.
[36] Li, Chun-Ta, and Cheng-Chi Lee, “A Novel User Authentication and Privacy Preserving Scheme with Smart Cards for Wireless Communications”, Mathematical and Computer Modelling, 2012, Vol. No. 55, Issue No. 1, pp 35-44.
[37] Jiang, Qi, Jianfeng Ma, Guangsong Li, and Li Yang, “An Enhanced Authentication Scheme with Privacy Preservation for Roaming Service in Global Mobility Networks”, Wireless Personal Communications, 2013, Vol. No. 68, Issue No. 4, pp 1477-1491.
[38] Wen, Fengtong, Willy Susilo, and Guomin Yang, “A Secure and Effective Anonymous User Authentication Scheme for Roaming Service in Global Mobility Networks”, Wireless Personal Communications, 2013, Vol. No. 73, Issue No. 3, pp 993-1004.
[39] Zhao, Dawei, HaipengPeng, Lixiang Li, and Yixian Yang, “A Secure and Effective Anonymous Authentication Scheme for Roaming Service in Global Mobility Networks”, Wireless Personal Communications, 2014, Vol. No. 78, Issue No. 1, pp 247-269.
[40] Memon, Imran, IbrarHussain, Rizwan Akhtar, and Gencai Chen, “Enhanced Privacy and Authentication: An Efficient and Secure Anonymous Communication for Location Based Service Using Asymmetric Cryptography Scheme”, Wireless Personal Communications, 2015, pp 1-22.
[41] Staddon, Jessica, Sara Miner, Matt Franklin, Dirk Balfanz, Michael Malkin, and Drew Dean, “Self-Healing Key Distribution with Revocation”, IEEE Symposium on Security and Privacy, 2002, pp. 241-257.

[42] Liu, Donggang, PengNing, and Kun Sun, "Efficient Self-Healing Group Key Distribution with Revocation Capability", In Proceedings of the 10th ACM conference on Computer and Communications Security, ACM, 2003, pp. 231-240.
[43] Blundo, Carlo, Paolo D'arco, Alfredo De Santis, and MassimilianoListo, "Design of Self-Healing Key Distribution Schemes", Designs, Codes and Cryptography, 2004, Vol. No. 32, Issue No. 1-3, pp 15-44.
[44] Blundo, Carlo, Paolo D'Arco, and Alfredo De Santis, "On Self-Healing Key Distribution Schemes", IEEE Transactions on Information Theory, 2006, Vol. No. 52, Issue No. 12, pp 5455-5467.
[45] Dutta, Ratna, and SouravMukhopadhyay, "Improved Self-Healing Key Distribution with Revocation in Wireless Sensor Network", In Wireless Communications and Networking Conference, IEEE, 2007, pp. 2963-2968.
[46] Dutta, Ratna, SouravMukhopadhyay, and Sabu Emmanuel, "Low Bandwidth Self-Healing Key Distribution for Broadcast Encryption", In Second Asia International Conference on Modeling& Simulation, IEEE, 2008, pp. 867-872.
[47] Daza, Vanesa, Javier Herranz, and GermánSaez, "Flaws in Some Self-Healing Key Distribution Schemes with Revocation", Information Processing Letters, 2009, Vol. No. 109, Issue No. 11, pp: 523-526.
[48] Han, Song, BimingTian, Mingxing He, and Elizabeth Chang, "Efficient Threshold Self-Healing Key Distribution with Sponsorization for Infrastructure-less Wireless Networks", IEEE Transactions on Wireless Communications, 2009, Vol. No. 8, Issue No. 4, pp: 1876-1887.
[49] Wang, Huaqun, and Yuqing Zhang, "Cryptanalysis of an Efficient Threshold Self-Healing Key Distribution Scheme", IEEE Transactions on Wireless Communications, 2011, Vol. No. 10, Issue No. 1, pp: 1- 4.
[50] Rams, Tomasz, and Piotr Pacyna, "Long-lived Self-Healing Group Key Distribution Scheme with Backward Secrecy", In Conference on Networked Systems (NetSys), IEEE, 2013 pp. 59-65.
[51] Chen, Huifang, and Lei Xie, "Improved One-Way Hash Chain and Revocation Polynomial-Based Self-Healing Group Key Distribution Schemes in Resource-Constrained Wireless Networks", Sensors, 2014, Vol. No. 14, Issue no. 12, pp: 24358-24380.
[52] Zheng, Yandong, and Hua Guo, "Cryptanalysis of an Improved One-Way Hash Chain Self-Healing Group Key Distribution Scheme", 2014.
[53] Huang, Qiang, JohnasCukier, Hisashi Kobayashi, Bede Liu, and Jinyun Zhang, "Fast Authenticated Key Establishment Protocols for Self-Organizing Sensor Networks", In Proceedings of the 2nd ACM International Conference on Wireless Sensor Networks and Applications, 2003, pp. 141-150.
[54] Tian, Xiaojian, Duncan S. Wong, and Robert W. Zhu, "Analysis and Improvement of an Authenticated Key Exchange Protocol for Sensor Networks", Communications Letters, IEEE, 2005, Vol. No. 9, Issue No. 11, pp: 970-972.
[55] Yoon, Eun-Jun, and Kee-Young Yoo, "An Optimizing Authenticated Key Exchange Protocol for Self-Organizing Sensor Networks", In Ubiquitous Computing Systems, Springer Berlin Heidelberg, 2006, pp. 537-546.
[56] Younis, Mohamed F., KajaldeepGhumman, and Mohamed Eltoweissy, "Location-Aware Combinatorial Key Management Scheme for Clustered Sensor Networks", IEEE Transactions on Parallel and Distributed Systems, 2006, Vol. No. 17, Issue No. 8, pp: 865- 882.
[57] Sun, Yan, and K. J. Liu, "Hierarchical Group Access Control for Secure Multicast Communications", IEEE/ACM Transactions on Networking, 2007, Vol. No. 15, Issue No. 6, pp: 1514 -1526.
[58] Traynor, Patrick, Raju Kumar, Heesook Choi, Guohong Cao, Sencun Zhu, and Thomas La Porta, "Efficient Hybrid Security Mechanisms for Heterogeneous Sensor Networks", IEEE Transactions on Mobile Computing, 2007, Vol. No. 6, Issue No. 6, pp: 663-677.
[59] Gu, Qijun, Peng Liu, Wang-Chien Lee, and Chao-Hsien Chu, "KTR: An Efficient Key Management Scheme for Secure Data Access Control in Wireless Broadcast Services", IEEE Transactions on Dependable and Secure Computing, 2009, Vol. No. 6, Issue No. 3, pp: 188-201.
[60] Banihashemian, Saber, and Abbas GhaemiBafghi, "A New Key Management Scheme in Heterogeneous Wireless Sensor Networks", In The 12th International Conference on Advanced Communication Technology (ICACT), 2010, Vol. No. 1, pp. 141-146.
[61] Guo, M. H., and D. J. Deng, "Centralised Conference Key Mechanism with Elliptic Curve Cryptography and Lagrange Interpolation for Sensor Networks", IET Communications, 2011, Vol. No. 5, Issue No. 12, pp: 1727-1731.
[62] Kakkar, Ajay, M. L. Singh, and P. K. Bansal, "Mathematical Analysis and Simulation of Multiple Keys and S-Boxes in a Multinode Network For Secure Transmission", International Journal of Computer Mathematics, 2012 Vol. No. 89, Issue No. 16, pp: 2123-2142.
[63] Guo, Ming- Huang, Horng- TwuLiaw, Meng- Yu Chiu, and Der- Jiunn Deng, "On Decentralized Group Key Management Mechanism for Vehicular Ad-Hoc Networks", Security and Communication Networks (2012).

[64] Li, Sujun, Boqing Zhou, Jingguo Dai, and Xingming Sun, "A Secure Scheme of Continuity Based on Two-Dimensional Backward Hash Key Chains for Sensor Networks", IEEE Wireless Communications Letters, 2012, Vol. No. 5, Issue No. 1, pp: 416-419.

[65] Chen, Chien-Ming, XinyingZheng, and Tsu-Yang Wu, "A Complete Hierarchical Key Management Scheme for Heterogeneous Wireless Sensor Networks", The Scientific World Journal, 2014.

[66] Yao, Wenbin, Si Han, and Xiaoyong Li, "LKH++ Based Group Key Management Scheme for Wireless Sensor Network", Wireless Personal Communications: 1-17.

[67] Mapoka, Trust T., Simon J. Shepherd, and Raed A. Abd-Alhameed, "A New Multiple Service Key Management Scheme for Secure Wireless Mobile Multicast", IEEE Transactions on Mobile Computing, 2015, Vol. No. 8, pp: 1545-1559.

[68] Jiming Yao, Tao Wang, Mingkai Chen, Lei Wang, Gejuan Chen, "GBS-AKA: Group-based Secure Authentication and Key Agreement for M2M in 4G Network", 2016 International Conference on Cloud Computing Research and Innovations, IEEE, 2016, pp: 42-48.

[69] ProbiditaRoychoudhury, BasavRoychoudhury, and Dilip Kumar Saikia, "Hierarchical Group Based Mutual Authenticationand Key Agreement for Machine Type Communication inLTE and Future 5G Networks", Security and Communication Networks, Hindawi, Volume 2017, Article ID 1701243, 2017, pp: 1-21.

[70] Muzammil M. Ahmad and Sibghatullah I. Khan, "Three-Tier Authentication and Secure Key Exchange Over Insecure Channel", International Conference on Big Data Analytics and Computational Intelligence (ICBDACI), IEEE, 2017, pp: 134-138.

[71] Yuxiang Feng,Wenhao Wang, YukaiWeng, and Huanming Zhang, "A replay-attack resistant Authentication Scheme for the Internet of Things", IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conferenceon Embedded and Ubiquitous Computing (EUC), 2017, pp: 541-547.

[72] Shubham Gupta,Balu L. Parne, and Narendra S. Chaudhari, "DGBES: Dynamic Group Based Efficient and SecureAuthentication and Key Agreement Protocol for MTCin LTE/LTE-A Networks", Wireless PersCommun, Springer, 2017, pp: 1-33.

[73] Prasanta Kumar Roy, KrittibasParai, Sathi Ball, and Bipin Kumar, "A New Enhanced Secure Anonymous Communication with Authentication and Session KeyAgreement in Global Mobility Network", Third International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN), 2017, pp: 109-113.

[74]Binu P K, Induja E, Monica Earnest, "Highly Secured Architectural Model for Web BasedApplications using 2-way Authentication Technique", IEEE, 2018, pp: 1006-1011.

[75]Balu L. Parne, Shubham Gupta, and Narendra S. Chaudhari, "SEGB: Security Enhanced Group Based AKA Protocol for M2M Communication in an IoT Enabled LTE/LTE-A Network", IEEE, 2018, pp: 3668-3684.