ISSN (Print) : 0974-6846
Indian Journal of Science and Technology, *Vol 11(46), DOI: 10.17485/ijst/2018/v11i46/132530, December 2018* ISSN (Online) : 0974-5645

A Systematic Review on Various Security Issues and its Mitigation Techniques in WMN

T. Senthil Kumar* and S. Prabakaran

SRM Institute of Science and Technology, Kattankulathur – 603203, Tamil Nadu, India;
senthilkumar.t@ktr.srmuniv.ac.in, prabakaran.s@ktr.srmuniv.ac.in

Abstract

Objectives: To delineate various security vulnerabilities and defence strategies involved in secure mobile communications. **Methods/Statistical Analysis:** Due to the enormous growth of mobile communication, there is also a fear on providing security and privacy preserving for users over the network. In this paper, the methodologies contributed for solving the security constraints of WMN have been discussed. Mainly, models based on Mutual Authentication, Authenticated Key Agreement (AKA), Elliptic Curve Cryptography based security employment and bilinear pairing techniques have been analyzed and described. Mention the methodology used; data base consulted, criteria for omission or inclusion; keywords used for data collection, period covered etc. **Findings:** The contribution involves in clear examination of methodologies satisfying major security requirements such as Authentication, Confidentiality, Availability and Integrity. Moreover, distinctive security constraints have been analyzed and mitigation techniques have been discussed for those security issues effectively. From the survey work, it is found that Mutual Authentication and Key agreement based Cryptographic conceits perform effectively in solving the security issues on WMN. **Applications/Improvements:** Further, this extensive analysis aims to elaborate the numerous unresolved issues and effective.

Keywords: AKA, Bilinear Pairings, ECC, Mutual Authentication, WMN

1. Introduction

In current scenario, the services and wide usage of Wireless Mobile Networks (WMN) have been propagating with the aim of competing with its fast demand escalation.[1,2] In accordance with the recent statistics published by the International Telecommunication Union in the year 2013,[3] almost fifty percentage of the world's population is adapted to the Internet and the number of mobile users worldwide is about 7 billion. On the other hand, it has also been stated in[4] that the rapid growth of using wireless devices are depraved for illegal cybercriminal actions, also includes computer hacking, online bullying, financial data stealing, malicious attacks, etc. Based on the Norton cybercrime report in the year 2012,[4] it is also reported that in every year these problems produce the direct currency loss of about 83 billion Euros for each 500 million users collided by cybercrime. Therefore, it is very vital to enhance the security on Wireless Mobile Communications to oppose and avoid cybercriminal activities and also to favour the increasing mobile users and Smartphone users worldwide.

In general, wireless networks affirm the OSI protocol architecture[5] that composed of various layers such as physical layer, MAC layer, network layer, transport layer and application layer. Each layer works on its own criteria and also the vulnerabilities and security related issues related to these layers are significantly protected in a detached manner to accomplish its security requirements at each layer. The security requirements mainly include Authentication, Confidentiality, Availability and Integrity.[6] The Figure 1 depicts the security aspects and its necessities in wireless networks. Authentication is the process provides the access over the network only to the authorized users. Confidentiality is to maintain the secrecy limit of the data or information transferred between networks. For avoiding falsification on the transmitted data, integrity is enforced. And finally, it is important for a good network to be available at anytime and anywhere, when it is needed by the authorized

**Author for correspondence*

users. As is well known, in order to provide security over communications, cryptographic techniques are widely used for preventing the data from unauthorized access and maintaining the confidentiality of the data shared throughout the communication. Though such techniques enhance the attainable confidentiality, it demands for some additional evaluative power and enforcing latency,[7] since there is some time is needed to be allotted for encryption and decryption.

For providing authenticity over mobile communication, multiple authentication methods are employed in different layers in simultaneous manner, which also includes MAC layer authentication and authentication process at transport and network layers. Specifically, in MAC layer, authentication is for preventing unauthorized access. Utilizing multiple authentication process at various protocol layers is a way for improving the wireless network security. Moreover, the main contribution of this work is to study and discuss about the assorted wireless attacks and its corresponding mitigation mechanisms. The remainder of this paper is organized as follows: Section 2 provides a deliberation on various security requirements in WMN, Section 3 narrates some effective mitigation techniques and finally, Section 4 concludes the paper with directions about future work.

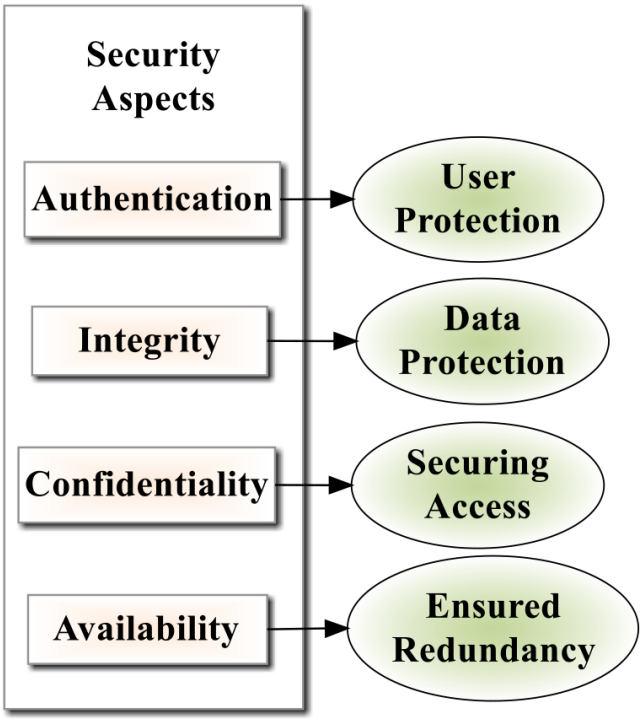

Figure 1. Security aspects in wireless networks.

2. Security Requirements in WMN

This section explains about the significant security parameters involved in wireless mobile network. Moreover, while framing the parameters, there are some design factors to be considered. As mentioned above, the security methodologies in wireless networks comprise authentication, authorization and encryption, in accordance to the security level, deployment complexity and communicational inactivity. The Figure 2 gives the pictorial representation of various design factors involved in framing a secure Wireless Mobile Network (WMN). It can be stated when theses design factors are achieved in a satisfied manner, the communication would be secure and privacy preserved.

Basically, in wireless medium, the data is shared or exchanged between some authorized users. But, due to the broadcasting nature of WMN, this sharing is open to vulnerabilities and some malicious threats. For protecting the wireless communications from various attacks like DoS (Denial of Service) attack, eavesdropping, node compromising, data falsification or duplication, there are some security requirements are specified.[8] For example, retaining data confidentiality is a significant security factor that denotes the ability of denying the data access from unauthorized users, that is, it prevents the eavesdropping attack. It is very obvious that, a secure wireless mobile communication should persuade the needs of Authentication, authorization, confidentiality, data integrity and availability, as described as follows.

- **Authentication:** It denotes to validating the exact identity of a particular node in a network in order to differentiate authorized and unauthorized users. A perfect solution for this in WMN, the specific pair of communicating hosts should execute Mutual Authentication (MA) initially, before accomplishing the link for information sharing.[9] Traditionally, a unique MAC address is used for authenticity in network layer which consist of a wireless network interface card. Authentication is incorporated in distinctive ways in network layer, transport layer and application layers.
- **Confidentiality:** It works on restricting the data access from unwanted users and also protecting the data from disclosing to unauthorized

entities.[10] Symmetric Key Encryption would be the perfect example or confidentiality. In that, the source node initially encrypts the original content with the help of secret key by using some encryption techniques and the key would be shared between the authorized destination nodes only. Once the destination node receives the encrypted content, it decrypts it using the provided secret key and extracts the original data. Hence, the eavesdroppers have no idea about the secret key and not able to interpret the encrypted data.

- **Integrity:** In Wireless communications, it is to be assured that the information shared over the network should be accurate and accountable throughout the life cycle without any modification, duplication or falsification of the content by any unknown users. Perhaps, the data integrity is desecrated by some insider attacks such as node compromising.[11] Such compromised nodes can be detected and revoked by accomplishing auto-code update and auto recovery process.
- **Availability:** Availability states that that the intended users should be able to access the network anywhere and anytime on demand. Sometimes DoS may happen that the authorized users may not be able to use the network and result in disappointing user experience.[12]

Hence, the fore mentioned factors are generally considered as the significant security requirements on the existing wireless networks that contain Wi-Fi, WiMAX, Bluetooth and LTE mobile standards.

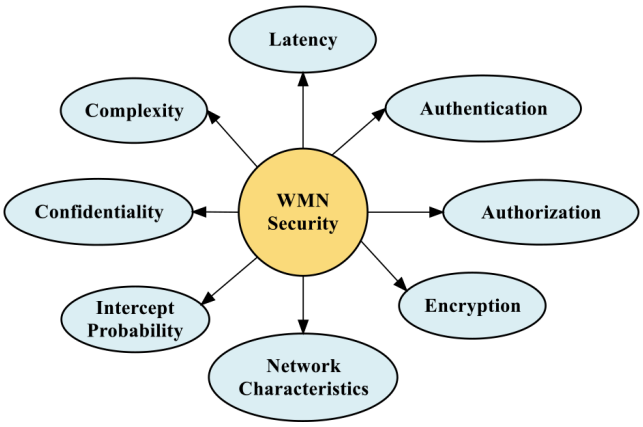

Figure 2. Design factors for WMN.

3. Mitigation Techniques

In this section, the existing efficient solution methodologies are being analysed for satisfying the security parameters of WMN. There are several techniques that are highly relying on Authentication and Key Agreement for building up the strongest security channel over communications.

Mutual Authentication Based Techniques

While designing the security protocols based on Authentication and Key Agreement, a novel model called The Dancing Signals (TDS) has been developed by.[13] The authors have been stated and proved that the TDS security protocol is robust and fast when compared to other models and it uses the CSI called Channel State Information. Moreover, the main idea behind TDS is doing the quantization process in separate manner, instead of making all end nodes to perform. That is, a single device or node is allowed to fix the arbitrary key and provides that to all other authorized devices in a confidential way. It comprises five steps which are as follows.

- Channel Sampling.
- S-Box Generation.
- Key Generation.
- Key Delivery.
- Information reconciliation.

During sampling, the CSI samples are evaluated by all the devices with the aid of some traditional synchronization protocol. Synchronization is needed till some of three nodes attain large number of samples commonly. Then, the S-box is being constructed. The key generation process has taken place and the keys are produced in a random manner through some existing algorithms. Following, the generated key is distributed to the intended user to extract the secret messages. Moreover, Information reconciliation is used by TDS to produce reliable keys on variant devices.

Another work[14] described about the Efficient Mobile Authentication Scheme that also be liable for low power devices. The process uses Elliptic Key Cryptography (ECC) for authenticity and it can fight against all the existing attacks, specifically, DoS. The authors named the overall process as EMAS (Efficient Mobile Authentication Scheme) that comprises two major phases, namely: 1. TDI (True Delegation Initialization) and 2. EMA (Efficient Mobile Authentication) and also a third elective phase called HLR (Home Location Register) offline Authentication (HOA).

3.1 Steps Involved in Phase 1 (TDI):

- HLR fixes the key usage constraint on a mobile station.
- Converts it into an element called and evaluates its hash value.
- A random number k is chosen and keys are generated by mapping it on correct point of representation on Elliptic curve.
- The key is distributed to Mobile Station.
- The Mobile Station (MS) accepts the delegation key.

3.2 Steps Involved in Phase 2 (EMA):

- MS selects two random numbers and creates a communication key.
- MS creates a certificate and compose a message S1 and opens a protocol by sending it.
- When the certificates are received by VLR, it checks for certain constraints, expiration timestamp and nonce consistency.
- VLR authenticates the particular mobile station, by decrypting the communication key sent by MS.
- HLR receives and forwards the communication key.

The authors have concluded the work with the statement that potential security measures are to be includes while designing a secure communication protocol for WMN and the Mobile Stations are to be authenticated in some effective ways. Kerberos based Authentication process is discussed in[15] that provides a deviated solution for centralized mobile authentication process. Kerberos based authenticity has been developed based on tickets for precise mutual authentication and incorporation of session key. It also concentrates on providing tokens in such a way that the mobile station can be accessible for the roaming partners of the home network as well as the earlier visited networks. As portrayed in Figure 3, most of the traditional protocols are centralized and when a mobile station hands over to another visiting network, the specific home network is needed to take part in authentication as given in the figure. In,[15] the authors proposed the design based on Kerberos protocol and provide inter- domain authentication and named it as Kerberos based Authentication for Inter-domain Roaming (KAIR). The KAIR based distributed authentication schema is presented in the Figure 4. Token based authentication is incorporated and the security analysis includes handling mutual authentication, key derivation and delivery, identity protection, man in the middle attack, compromised tokens, brute-force attack and so on. The authors concluded with the description that the process does not involve in providing authorization and integrity. In further improvements, that could be included based on policies and billing schemes.

In,[16] Femtocells are used to improve the service coverage of a particular network; with that mutual authentication protocol is induced for providing secure way or communication. For that, Rapid Development Authentication Protocol (RDAP) has been proposed and implemented. Moreover, the protocol defends the mobile network from attacks such as injecting attacks, packet sniffing, Sybil attack, eavesdropping and DoS (Denial of Service). RDAP comprises three phases namely, scanning, mutual authentication and accomplishment of secure connection. Initially, in scanning, the User Entity (UE) scans the Quick Response (QR) code of the femtocell. The code contains secret keys for encryption (ke) and authentication (ka) in 128-bit. Following the scanning process, mutual authentication involves in key exchange by using Diffie-Hellman. AES and SHA-1 is used for encryption for preventing the network from tempering attack. The user entity and the femptocell share the data among themselves or mutual authentication. Then, femtocell sends a mobile identity request as follows, for managing with Access Control List (ACL).

Femtocell→ Mobile: Identity Request.

The mobile node responded by generating 1028 bit random number, nonce and encrypted the message (ms) with the secret key (ke). The total response is hashed with the authentication key (ka). Then, the secure connection accomplishment has been made with the femtocell and the mobile device that ensures reliability and data accountability.

Mutual authentication for secure mobile communication has been handled in a distinctive way in.[17] The authors have considered three entities such as biometric attribute of the subscriber, subscriber's password and SIM for secure 4-G communications. There are four phases involves in this process such as:

- Subscriber Enrolment Phase.
- Subscriber Authentication Phase.
- Network Authentication Phase.
- Subscriber Password Change Phase.

In first phase, the subscribers are required to be enrolled themselves to a particular server by creating its own identity, biometric property and a password. On preceding this, each subscriber is provided with a SIM. In next phase (Subscriber Authentication Phase), the network verifies the subscriber's authenticity while starting each communication. This phase is executed at once a call connection is established through the network. The network authentication is to check whether the connection is established with the desired network or not. The last phase of this process is accomplished in on-demand manner, when there is a need of changing or replacing a subscriber's password by them. On the other side, the paper had no discussions about the other security constraints of the mobile networks.

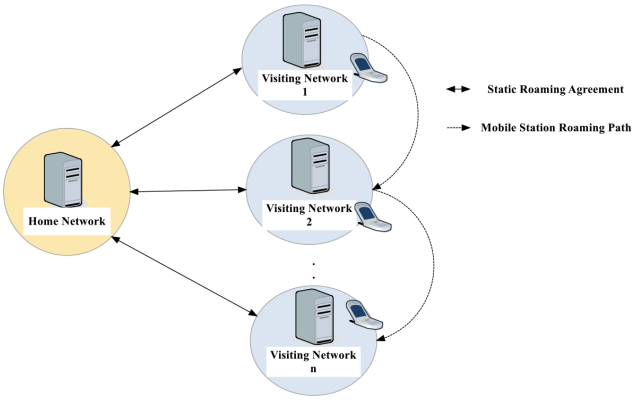

Figure 3. Existing centralized schema.

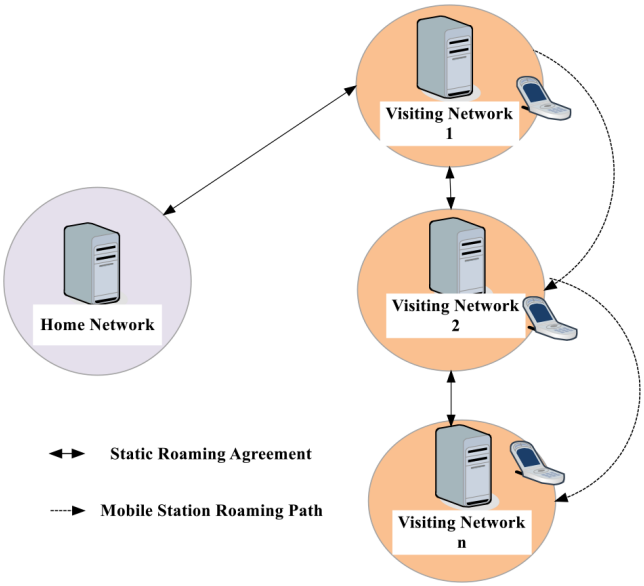

Figure 4. KAIR based distributed schema.

3.3 Authenticated Key Agreement (AKA) based Protocols

In[18] have developed a secure authentication mechanism based on the combination of public key cryptosystem with some efficient hashing techniques. Moreover, the mechanism uses SEQ (Sequence Number) for avoiding convoluted synchronizations. The main contribution of the authors to frame the UMTS (Universal Mobile Telecommunication System) based AKA (Authentication and Key Agreement) protocol. It accomplishes three goals: Mutual Authenticity between the network and subscriber, determination of cipher and integrity keys for authentication and deliberates assurance to the user. The following Figure 5 gives the working process of authentication in AKA protocol in simple way. Moreover, the basic needs of AKA protocol are given as follows:[19]

Mutual Authentication: Two parties involve in a particular communication ensure that they are authenticated to each other and sending information to the correct party/entity.

Key Verification: After allocation of the session key, it should be verified by both the parties.

Ideal Forward Secrecy: If there is session key is conceded, it is to be assured that the attackers cannot predict the previous keys.

Known Key Security: It ensures that the session key produced by each session is distinct and non-similar.

Key Control Security: This property is to avoid the parties involving in key value determination.

Session Key Security: The knowledge about the session key should be avail only to the parties involved in that communication.

Based on AKA, in,[20] the authors have proposed an efficient protocol named Identity based Two-Party Authenticated Key Agreement (ID-2PAKA), uses Elliptic Key Cryptography. The protocol concentrates on avoiding public key certificate, bilinear pairing and MTP (Map-to-Point) hash free realization. Moreover, the process uses three entities such as PKG (Public Key Generator) and the two parties involved in communication. The authors have used the traditional BAN logic model for providing formal security throughout the communication. The authors have divided the working strategy of the pairing free AKA protocol as setup phase for secure key generation, extract phase is to generate identity for the indeed users and the key agreement phase is for the successful establishment of session keys for each session. The results are analyzed

by made the discussion with various attacks such as key replication attack, known key attack, key compromising attack and so on.

Secure Authentication and Key Agreement (SAKA) protocol[21] for GSM (Global System for Mobile Communication) Network. The protocol effectively reduces the consumption of bandwidth between the HLR and VLR and also the overloaded storage among them. This avoids the synchronization requirement between the mobile station and the home network. The SAKA protocol produced lowest communication overhead when compared with the protocol in practice. The main contributions of the protocol is said to be providing mutual authentication, generating key agreement, maintaining key freshness among mobile station VLR and finally, ensuring confidentiality. The same Mutual Authentication and Key Agreement have been implemented for Long Term Evolution (LTE) technology in user-user security manner.[22] In this model, the network takes the responsibility of proxy and the third party for providing the security archetype with more accountability and security. For attaining this, verification proxy signature is incorporated in accordance with bilinear pairing. Moreover, some adaptations has also made with the basic security algorithms and the design architecture of LTE. The following Figure 6 shows that handshaking flow of LTE-AKA protocol. In the flow, HSS represents the Home Service Server, MME stands for Mobility Management Entity and UE for User Equipment. The direction of flow denotes as follows:

- Sending Service Request using Service Network ID.
- Exchanging Keys and device parameters.
- Receiving Service Response.
- Exchanging data via secure link.
- Sending service request using Home network ID.
- Service response using the ID of Home Network.

The AKA protocol design on the basis of Simple Password Exponential Key Exchange (SPEKE) has been induced in.[23] With additional effort, the size of the data exchanged between the UE and HSS is considerably reduced and simultaneously, the authentication delay and the storage consumption are minimized. The authors have used AVISPA tool for formal key verification.

In an improvised way, the recent paper on AKA has introduced Hierarchical Group based Mutual Authentication and Key Agreement (HGMAKA).[24] It forms a HetNet that comprises femtocells, mobile femtocells, macrocells and the required network devices. For performing multiple operations, the architecture is organized as three tiers. The first tier performs data accumulation from MTCD (Machine Type Communication Device) and the second tier assembles the data gathered from various MTCDs. The third tier ensures secure communication channel to the core network. Moreover, the HGMAKA protocol algorithm contains two phase:

- Aggregate Generation Phase.
- Group based Mutual Authentication and Key Agreement phase.

In phase 1, the authentication messages are combined and taken to the second tier and preceded by the third and integrity checking has also been done with each tiers. In phase 2, the Home Network approves all group members simultaneously from the aggregated results and the MTCDs validate the MME and the Home Service Server through the unique secret key exchanged between the MME and the machine type communication device. The security analysis has taken place with the examination of various attacks long with the proposed HGMAKA protocol.

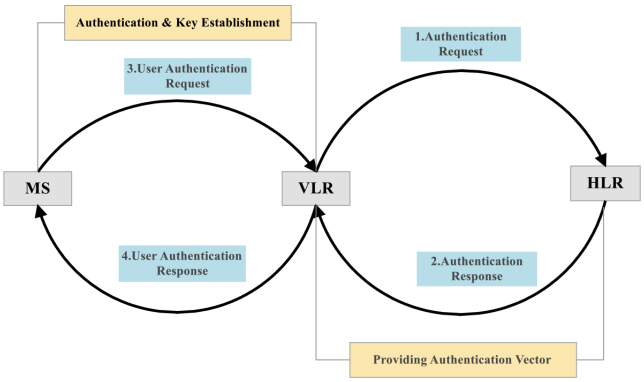

Figure 5. Basic design of AKA protocol.

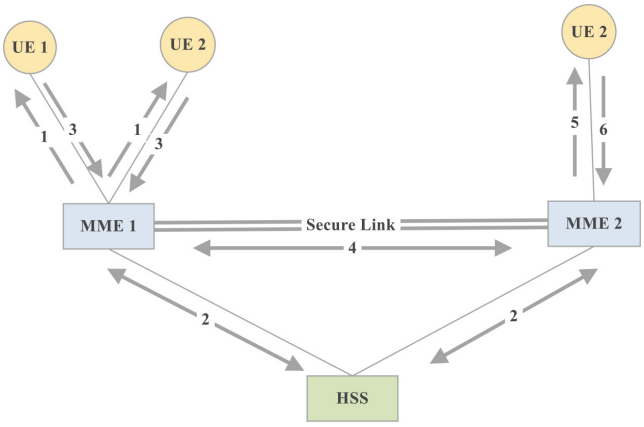

Figure 6. Handshaking flow of LTE-AKA protocol.

4. Summary and Conclusion

In this study, an effective survey is presented about the security challenges in wireless mobile networks and the mitigation techniques for providing Authentication, Confidentiality, Integrity and Availability of wireless communications against various malicious attacks. Moreover, distinctive security constraints are studies and issues have been adequately examined through this survey work. The mitigation techniques described by various authors based on some cryptographic conceits such as Mutual Authentication, Authenticated Key Agreement, ECC based Scalar Point Multiplication, MME Authentication, proxy signature Verification, etc. By analyzing all, it can be stated and recommended that Mutual Authentication and Key Agreement based protocols have produced convincing results with reduced computational cost and time.

Hence, the main intention of the survey has been attained and a better schema for secure communication based on Mutual Authentication and Key Agreement protocol will be framed as the future work. The results would be examined with various attacks and are expected to be achieving reduced computational complexity, cost and time. The direction to future work is to develop an enhanced privacy preserving model for providing highly secure communication over WMN.

5. References

1. El Sawy H, Hossain E, Haenggi M. Stochastic geometry for modeling, analysis and design of multi-tier and cognitive cellular wireless networks: A survey. IEEE Communications Surveys and Tutorials. 2013; 15(3):996–1019. https://doi.org/10.1109/SURV.2013.052213.00000
2. Aliu O,Imran A, Imran M, Evans B. A survey of self organisation in future cellular networks. IEEE Communications Surveys and Tutorials. 2013; 15(1):336–61. https://doi.org/10.1109/SURV.2012.021312.00116
3. The World in 2013: ICT facts and figures. 2013. https://www.researchgate.net/publication/259255435_The_World_in_2013_ICT_facts_and_figures
4. The 2012 Norton cybercrime report. 2012. https://www.slideshare.net/marianmerritt/2012-norton-cybercrime-report-14175700
5. Rashid MM, Hossain E, Bhargava VK. Cross-layer analysis of downlink V-BLAST MIMO transmission exploiting multiuser diversity. IEEE Communications Surveys and Tutorials. 2009; 8(9):4568–79.
6. Kolias C, Kambourakis G, Gritzalis S. Attacks and counter measures on 802.16: Analysis and assessment. IEEE Communications Surveys and Tutorials. 2013; 15(1):487–514. https://doi.org/10.1109/SURV.2012.021312.00138
7. Xiao Y, Chen HH, Sun B, Wang R, Sethi S. MAC security and security overhead analysis in the IEEE 802.15.4 wireless sensor networks. EURASIP Journal on Wireless Communications and Networking. 2006. https://doi.org/10.1155/WCN/2006/93830
8. Ma D, Tsudik G. Security and privacy in emerging wireless networks. IEEE Wireless Communication. 2010; 17(5):12–21. https://doi.org/10.1109/MWC.2010.5601953
9. Jiang Y, Lin C, Shen X, Shi M. Mutual authentication and key exchange protocols for roaming services in wireless mobile networks. IEEE Transaction Wireless Communication. 2006; 5(9):2569–77. https://doi.org/10.1109/TWC.2006.05063
10. Stalling W. Cryptography and network security: Principles and Practices. 3rd ed. Englewood Cliffs, NJ, USA: Prentice-Hall; 2010.
11. Lin X. CAT: Building couples to early detect node compromise attack in wireless sensor networks. IEEE Global Telecommunications Conference; 2009. p. 1–6. https://doi.org/10.1109/GLOCOM.2009.5425922
12. Huang H, Ahmed N, Karthik P. On a new type of denial of service attack in wireless networks: The distributed jammer network. IEEE Transaction Wireless Communication. 2011; 10(7):2316–24. https://doi.org/10.1109/TWC.2011.052311.101613
13. Xi W, Qian C, Han J, Zhao K, Zhong S, Li XY, Zhao J. Instant and robust authentication and key agreement among mobile devices. CCS '16 Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security; 2016. p. 616–27. https://doi.org/10.1145/2976749.2978298
14. Tang C, Oliver D. An efficient mobile authentication scheme for wireless networks. IEEE Transactions on Wireless Communications; 2007. p. 1–9.
15. Shrestha AP, Choi DY, Kwon GR, Han SJ. Kerberos based authentication for inter-domain roaming in wireless heterogeneous network. Computers and Mathematics with Applications. 2010; 60:245–55. https://doi.org/10.1016/j.camwa.2010.01.019
16. Naqasa T, Hasan A, Isfaq A, Shabir K, Yasin A, Mujhaid U, Nazam-ul-Islam, Hasen Mehmood. Mutual authentication protocol for LTE based mobile networks. IEEE International Conference on Open Source Systems and Technologies (ICOSST); 2012. p. 1–4. https://doi.org/10.1109/ICOSST.2012.6472836
17. Bhattacharjee PK, Kumar R. Mutual authentication technique applying three entities in 4-G mobile communications. International Journal of Computer Theory and Engineering. 2011; 3(6):732–7. https://doi.org/10.7763/IJCTE.2011.V3.401

18. AL-Fayoumi M, AL-Saraireh J. An enhancement of authentication protocol and key agreement (AKA) for 3G Mobile Networks. International Journal of Security (IJS). 2011; 5(1):35–51.
19. Lo JW, Lee CC, Hwang M, Chu Y. A secure and efficient ecc-based aka protocol for wireless mobile communications. International Journal of Innovative Computing, Information and Control. 2010; 6(11):1–9.
20. Hafizul Islam SK, Biswas GP. A pairing-free identity-based two-party authenticated key agreement protocol for secure and efficient communication. Journal of King Saud University – Computer and Information Sciences. 2017; 29:63–73.
21. Saxena N, Chaudhari NS. SAKA: A secure authentication and key agreement protocol for GSM networks. Springer Publications, CSIT. 2013; 1(4):331–41.
22. Ramadan M, Li F, Xu CH, Mohamed A, Abdalla H,Abdalla A. User-to-User mutual authentication and key agreement scheme for LTE cellular system. International Journal of Network Security. 2016; 18(4):769–81.
23. Alezabi KA, Hashim F, Hashim SH, Ali BM. An efficient authentication and key agreement protocol for 4G (LTE) networks. IEEE Region 10 Symposium; 2014. p. 502–7.
24. Roychoudhury P, RoychoudhuryB, Saikia DK. Hierarchical group based mutual authentication and key agreement for machine type communication in LTE and Future 5G networks. Hindawi Security and Communication Networks. 2017. p. 1–21.