SECURITY CHALLENGES AS A FACTOR AFFECTING THE SECURITY OF MANET: ATTACKS, AND SECURITY SOLUTIONS

Dr.Nabeel Zanoon[1], Dr.Nashat Albdour[2], Dr.Hatem S. A. Hamatta[1], and RashaMoh'd Al-Tarawneh[1]

[1] Department of Applied Science, Aqaba University College/Al-Balqa Applied University, Aqaba, Jordan
[2] The Department of Electrical & Computer Engineering, Tafila Technical University, Tafila Technical Universities, Aqaba, Jordan

ABSTRACT

The Ad Hoc mobile network (MANET) is a wireless network with properties which may constitute challenges and weaknesses before the security progress in MANET network. It causes weakness in security, which leads to increased attacks on MANET. In this paper the challenges and attacks likely to threaten MANET will be investigated. As a corollary, security solutions will be discussed, the relationship between them will be concluded and architectural security solutions in MANET will beproposed.

KEY WORDS

MANET, Ad Hoc, Challenges, Attacks, Security Solutions, wireless.

1.INTRODUCTION

Nodes are linked to each other by a wireless medium where each node makes an end guided to all nodes connected to a network. [1] MANET is the network which consists of a collection of devices or nodes connected with one another without the help of any central administrator. It can form a dynamic network for the exchange of data without the use of any others network with fixed dynamic infrastructure. Any node can be connected to the networkbywireless medium dynamically, but at the same time it represents the role of the node and routers. The Topology MANET is renewed, because the nodes change and enter in the network and leave network continuously. However, MANET provides advanced, renewed and constant technology, but it faces challenges that threaten its security [2]

The concept of security for (MANET) means protocols security to which you subscribe and deal with it in order to protect it from threats. In order for MANET to do its core business, which is the exchange of data between the related and connected nodes, [3] there are those who threaten and attack the security of MANET from outside and also from inside. The attacks are in two levels;

DOI : 10.5121/ijnsa.2015.7301

the first level is the attack on the basic mechanisms such as guidance, while the second level of the attacks threatens the security that protects the MANET network. [4]

MANET has two dimensions in protection: the first dimension is protection of guidance operations through communication between the nodes; and the second dimension is the protection of the data to be exchanged. The security solutions to protect MANET are in the level before the attacks so as to form a defense line that provides protection. [5] But MANET characteristics pose challenges to the development of security solutions, because of a variety of attacks exploiting vulnerabilities in MANET caused by challenges. [6]

Wireless MANET is considered more vulnerable to attacks compared with wired networks because there are several challenges that will be studied in this paper. The security in MANET is an important issue, because in MANET communication is in groups.Also senders and receivers are multiple in a complex way compared with the case of a unicast. Most solutions for unicasts are ineffective with the multicast [7] in providing a secure connection in such a changing environment as well as protection against specific threats and attacks. There must be a different architectural and security plans. [8] In this paper we will highlight the security architecture design and feature analysis, as well as factors of insecurity, security threats and the relationship between them in MANET. Security challenges are considered obstacles, for they are threatening the security of MANET network, and there are several challenges facing the security of MANET.

2.CHALLENGES IN MANET NETWORK

The challenges facing the (mobile ad hoc) networks are a concern for the design and communication processes in the network. Some MANET network characteristics pose challenges in front of security solutions in MANET network [9].

2.1.Infrastructure And Routing

The nature of the network is one of the problems that stand in front of MANET network security. The nature of MANET network is open and its topology is mobile not fixed. Direction is considered an important issue for security because the nodes work as a guide. Guides are free to move randomly and organize themselves without any bases [10] The basis of the work of (Ad hoc) network is independent of any infrastructure, and this leads to any viable classic list of the application on the certification and on servers line. This leads to no classical applicable solutions based on certification and the line servers which have no such clear and secure borders in the cellular network, if compared with other networks such as wired network [11]. We conclude that the network topology affects the performance of the network. The nodes in the network are constantly moving, changing the nodes from time to time and this makes it difficult to predict the patterns of distribution and dealing with route decisions.

2.2.Mediums of wireless communication

By nature the MANET network is a wireless network. Signals are transmitted between network nodes through a joint medium. The wireless medium is considered extensive and unrestricted with any limits of any open centre. It is apt to the influence of external signals. Accordingly, it is regarded less reliable from wired means of communication [12]. The medium in wireless MANET is multi-hops, for it is affected by the overlap between neighbouring devices [13]. In other words, the wireless joint medium makes MANET more vulnerable to attacks than others. This is causing a number of attacks that affect MANET.

2.3.Energy consumption

The cellular phones that subscribe in (MANET) network rely on energy sources such as batteries, which is a problem in wireless networks. A device in (MANET) works as a director which constantly communicates with other devices, and this energy plays an important role [14].

2.4.Scalability

The MANET network is expandable and scalable in terms of the number of nodes and topology. The potentiality of development means the network's ability to provide service to the nodes connected to a network, taking into consideration the size of the network and the increasing number of nodes from time to time [15]. The size of the network and the number of nodes connected to the network plays an important role in control mechanism. It is a challenge for the network security. Therefore, a security mechanism is able to protect the network must be provided, regardless of the size and number of nodes in the network [16].

2.5.Bandwidth

Bandwidth in MANET network is regarded a difficult problem, because it is shared between the neighbouring hosts, while individual host has no knowledge about the other traffic of the neighbouring hosts [17]. In MANET network the routing tables of nodes are updated repeatedly and continuously, and this leads to the consumption of a large amount of bandwidth, which represents an obstacle for the network as it leads to a decline in the ability of the network to send and receive data. [18]

2.6.Software and applications in devices

Developed devices in MANET are used to access e-mail, various applications and data, games, etc. However companies are struggling between satisfying the needs of the subscribers and influencing the security situation [19]. Programs on the machine may be out of date, which is regarded as a sign of weakness which may be exploited by attackers [20].The Social networking programs contain user information and are used to communicate with others without restrictions and control.

3.SECURITY THREATS AND ATTACKS IN MANET NETWORK

There are several types of attacks which threaten the security MANET network. There are two types of attacks that threaten the security MANET network, negative and effective. The negative attacks are based on eavesdropping and spying on data traffic in the network and acquire important confidential information, while effective attacks affect the guidance protocols through malicious nodes as fake nodes based on misleading the data traffic by fabricating false guiding information [21]. The MANET network is a global network that provides essential services to users. Therefore it should provide confidentiality, safety and protection of the information from any attack. The attacks and their impact on MANET Security Network will be discussed as follows:

3.1.Types of attacks

Attacks are divided according to the attacker's site into two types; an external attack where the attacker is not from the network but is located outside the network. As for internal attack, the attacker enters as a node in the network and participates in the activities of the network as well, but it plays the role of a cheater by sending some phantom packages that mislead the course of the traffic in the network [22]. In the MANET network there are negative and effective attacks. Negative attacks in the MANET network use spying mechanism on information by stealing confidential data and tracking transmitter packs. Nevertheless, they do not implement any action which affects traffic and guidance. They are unknown and difficult to detect and recognize, and unlike effective attacks they can be detected and identified easily. They are based on the change in the track and affect the data traffic through the confusion on the network, and are located in different layers of the online model as shown in table (1) [23].

Table 1. The impact of the attacks on the MANET by layers: model OSI. [27] [26] [25] [24]

Layers	**Attacks**	**Effects**
Physical	**Eavesdropping**	It spies on data packets, steals important information, and puts itself between the parties to contact.
	jamming attack	It sends fake signals and interferes with effective communication. It affects the performance of the network by reducing the capacity of the package and delaying the delivery of packets, and the packets may reach damaged.
Data Link	**Traffic Analysis**	It is based on the track and analysis of the flow of traffic so as to know the network scheme, leading to detect nodes and have access to them.
	Malicious behavior of nodes	It is based on disabling the work of guidance protocols, and occupies a place between nodes.
	Monitoring	It is based on access to confidential data without being able to change or amend them.
Network	**Black hole attack**	It occurs during the implementation of the packet guiding process. It uses a guidance protocol so as to identify itself as the course of authentication to the target node. It creates a reply message to so that it takes the shortest path to the goal. It uses a fake way to reach the goal.
	Rushing Attack	It sends a request to the nodes that will be attacked, and the nodes reply to the real demand, and then the fake demand is approved, and thus the attacker comes into contact.
	Sinkhole attack	It is based on misleading the data traffic path and exploits it for its benefit in changing or destroying the confidential information.
	Gray Hole Attack	It is based on dropping messages to mislead the path to the destination, and here is an ambush of where to drop the package.
	replay attack	It is based on a repeat of the attack on data packets so as to inject the traffic that has been captured in the past, leading to mislead the guiding path in the MANET network.
	resource consumption	Is is based on the discovery of the path or re-directing unnecessary ones repeatedly and continuously.
	wormhole	It is represented in the cooperation between two attacking nodes. The first attacker picks a package and to the other attacker by using a high-speed medium.
	Byzantine attack	It consists of a set of nodes and is collectively sets up guide rings, and it also guides packets in worst tracks
	GRAY HOLE attack	It misleads the track and drops packets, which can be regarded as a declaration of itself as the right track so as to drop packets.
Transport	**SYN flooding attack**	It comes in the middle of the contact by sending SYN to the target node and exploits a response from the ACK target node.
	Session hijacking	It is based on the exploitation the address of the IP target by identifying the correct serial number. It works to stop service from the target node as if they were non-existent in the network.
Application	**Repudiation attack**	It eavesdrops and then rejects or denies knots a participation node in contact after it had contributed in part or whole contact.
	Malicious code attacks	It attacks operating system and applications which reside as viruses, worms and spyware, and Trojan horse.

4.SECURITY REQUIREMENTS FOR MANET

The task of providing security in the MANET network is a key matter in order to protect the services that are exchanged between the nodes. It is necessary to find security solutions for MANET network where security services such as confidentiality and integrity, non-repudiation, authentication, authorization and anonymity, are available. These security services are a fundamental requirement in security solutions in MANET network [28]:

- Confidentiality: to maintain the confidentiality of any information or data, and never be disclosing it to unauthorized parties, because the unauthorized parties threaten MANET network security.
- Integrity: protection of message data during transmission, that is, the data are not to be changed during transmission.
- Availability: it is based on maintaining the survival of network services while working on the denial of service attacks.
- Non-repudiation: it ensures that the sender of the message cannot deny sending a message that after sending it, that is, to guarantee showing the identity of sender.
- Authentication: to ensure the identity of the nodes connected to the network, that is, authentication when connecting to the network.
- Authorization: it is a mechanism for defining the powers to gain access to certain resources, that is, control over how to access the network.
- Anonymity: keeping personal information on a node, and not distributed by the node itself or the system software, that is, contact is unknown [29].

5.SECURITY SOLUTIONS FOR (MANET) NETWORK

The MANET network provides communication between different nodes; these nodes do the functions of the basic network, including sending, receiving, and forwarding packets. Nodes may be exposed to attack during the communication and performing the functions of the network. The network must be protected, and to ensure the security of the network a security mechanism has to be put to counter attacks that threaten the security of the network. In MANET network there are two types of security mechanisms that help protect MANET network of the attackers, including the preventive mechanism and reaction mechanism. The preventive mechanism works as the first line of defence in the protection process through the use of certain techniques that help to protect the network from the dangers. These methods include authentication, access control, encryption and digital signatures. The reaction mechanism represents the second line of defence and it uses schemes such as intrusion detection system (IDS) to detect misuse and anomalies [30]. Having studied the attacks that threaten MANET network and known the security requirements, we conclude that complete security solution requires the presence of both prevention and detection mechanisms and reaction in MANET.

5.1.Characteristics of security solutions

The security solutions are based on network protection and raising the level of security in the MANET network. As a corollary, there has to be some properties available in the proposed network security solutions in MANET including:

- The security solution must be applied through the individual components for collective protection of each network.
- The security solution must include all layers, as these layers work complementarily.
- The security solution must provide the ability to avoid threats from both internal and external parties.
- The security solution must apply all security mechanism including prevention, detection, and interaction [31].

5.2.Architectural security solutions for MANET.

In this paper security in MANET has been studies by investigating the challenges, attacks and security requirements. Accordingly, an architectural design shows each component and its role in reaching a security solution to a problem of defining the security of MANET. MANET network, like other networking systems, requires several things that must be taken into account when designing MANET network or when proposing a security solution. Any security solution must include security mechanism.

From figure 1, it is noticed that any connection between two nodes is made in a coherent communication is done through another node. During contact some challenges are encountered which is a sign of weakness in the level of protection, and this helps to give opportunities for attackers of MANET whether from the outside or from the inside. Solutions must be found to protect MANET network based on the security requirements and security mechanism in order to reduce and avoid the challenges, and this leads to reduce and avoid attacks. Hence we strengthen and raise the level of protection by a strong security wall against attacks. In this architecture each component affects the other components.

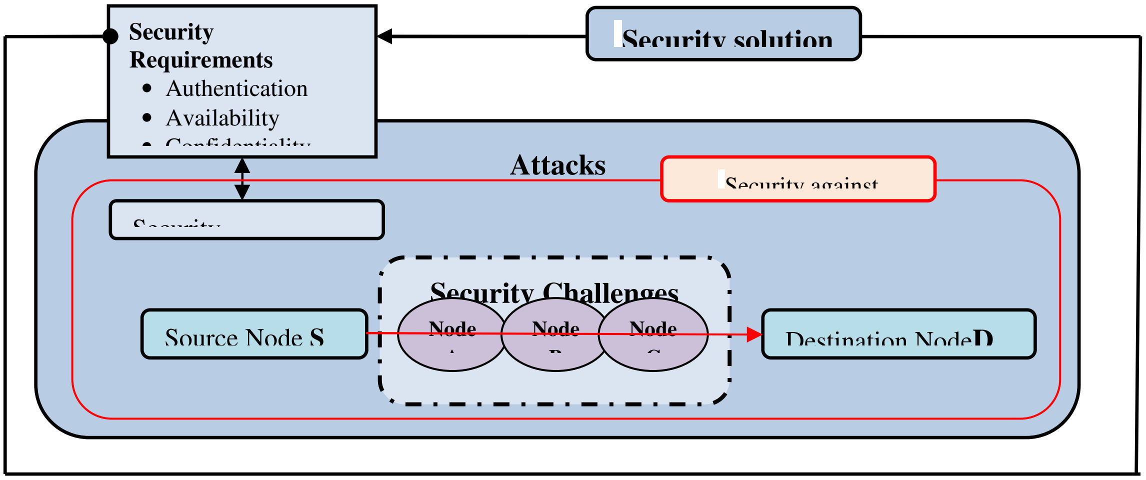

Figure 1. Architectural Security Solutions in MANET

5.3.The proposed security solutions

The security mechanism in MANET requires security solutions so as to build a security wall to protect MANET against risks and attacks that may be exposed to it. The attacks occur when security is weak which results in the challenges which stand in the development of security solutions. The challenges must be investigated and avoided in order to provide a safe environment devoid of threats and attacks. In this study some of the security solutions are suggested in table 2.

Table2. The Security Solutions against the Attacks on MANET

Challenge	Attacks	Solutions
• Infrastructuraland Routing • The Wireless Media • Power Consumption • Scalability • Bandwidth • application on devices	Eavesdropping jamming	Works by way of spread spectrum
	Traffic Analysis Malicious behavior of Nodes Monitoring	Works to correct the error in the debug code
	Black Hole Sinkhole Gray Hole WormHole GRAY HOLE Black Hole Rushing Replay Resource Consumption Byzantine	Works on authentication mechanism of sources and integrity and secure guiding protocols
	SYN flooding Session hijacking	Works on the authentication mechanism and ensuring contact between the two parties by using (SSL, TLS, PCT) encryptions
	Repudiation Malicious code	Work on the detection and prevention of the virus through the use of firewalls, IDS

6.LEVELS OF SECURITY IN MANET NETWORK

Contact between any two parties in MANET consists of a node which may be a cellular and a wireless transport medium and routing protocols and packet data, while challenges include all the components of MANET, as the attacks threaten the security of all MANET components. MANET network is made up of communication between several mobile devices, which constitute points of connection. The exchange of packets takes place through the wireless medium network. MANET is different from the other networks in that it contains no cellular base stations or access points, which represent the central administration.

6.1.Node level: The nodes represent a point of contact in MANET. They are distinguished by certain characteristics each of which represents a challenge to the security mechanism in MANET:

- Nodes in MANET are connected together via a wireless medium.
- The nodes work as a host device and router at the same time.
- Nodes in MANET share the same medium.
- Nodes in MANET use multiple-hop communications.
- Nodes in MANET move freely and automatically.
- Nodes in MANET have a limited capacity in terms of power, memory, etc.

6.2.The level of transport medium: It represents the line through which data pass between the contact points in MANET. The medium of the transport is characterized by characteristics that represent a challenge to the security mechanism in MANET:

- The medium of transfer is common in MANET.
- All points in MANET medium may transmit at any time.
- The medium of transfer is protected from any external signal.
- The medium of transfer has different time periods and asymmetric characteristics of spread.

6.3.The level of data packets: The data move between the contact points in MANET in the form of packets of data. The packets are characterized by qualities of challenging the security mechanism in MANET:

- The packets contain a group of information on the source node, the destination node and on routing packets.
- The routing tables in each node are stored for the routing process.
- The packets size increases with continuous change of the size of the network.

6.4.The level routing protocols: The path and nodes in MANET are determined by routing protocols. The protocols are characterized by qualities which represent each challenge in front of security mechanism in MANET

- Routing protocols are divided into two parts; the first are proactive protocols which are characterized by proactive examination of links to modify routing tables and emotional reaction when a problem is detected.
- Routing protocols are based on updating information in guidance table either periodically or upon request.
- Routing protocols use algorithms in determining the best path for routing packets.

7.RELATIONSHIP BETWEEN CHALLENGES, ATTACKS AND SECURITY IN MANET

It has been shown in the architectural security solutions for MANET that the security mechanism in MANET is integrated. Each component depends on the other component, and therefore we conclude that the relations between the security components in MANET, as shown in Figure (2) show that the security requirements are just a starting point when we want to put security solutions. The relationship is as follows: when the level of security is low, it is attributed to the challenges facing the development of security solutions, leading to the increase in attacks. On the other hand, when challenges are few, there are fewer attacks on the MANET. This is an indicator of raising the level of security in MANET. The relationship shows that the challenges are an obstacle to the development of some security solutions for MANET network.

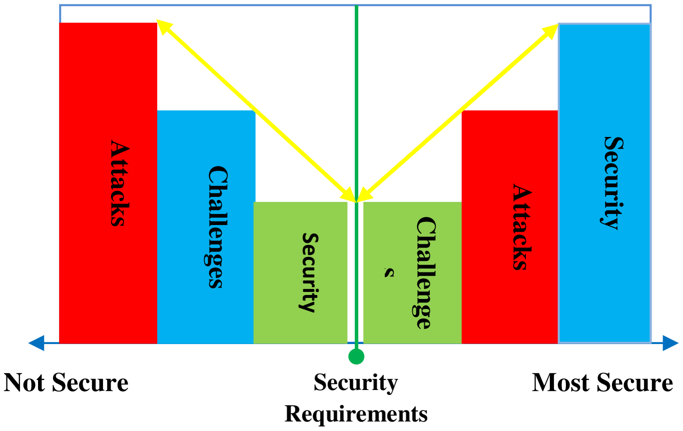

Figure 1.Relationship between challenges, attacks and security in MANET

Security mechanism in any network system is affected by attacks that penetrate the wall of network security through challenges, which is a gap in the security. MANET is affected by the attacks through the challenges of security. Table 3 shows the relevance of the effect of each of the challenges and attacks on MANET components.

Table 3.The Link between the Components, Challenges and Attacks in MANET

Attacks	**Components In Security**	**Challenges**
Resource consumption	Node: Mobile Devices	Power Consumption, Software and application, Infrastructural
Sinkhole, Gray hole, Wormhole, Flooding, Replication	Data: packets	Bandwidth, Scalability, Infrastructural, Wireless Media, Cooperativeness
Byzantine, Gray hole, Black hole, Wormhole, Sinkhole, Resource consumption, Routing, Flooding, SYN flooding	Route: routing Protocol	Scalability, Infrastructural, Wireless Media, Cooperativeness, Power Consumption
SYN flooding, Eavesdropping Jamming, Active Interference	Media: wireless	Bandwidth, Wireless Media. Power Consumption

8.CONCLUSION

In any communications system, there are some challenges, and these challenges are considered an indicator of the security gaps which generate weakness in the system protection and are vulnerable to attacks. The MANET network, like other networks, faces some of the challenges that have been studied in this paper. They form a gap in the firewall to MANET. However, security solutions must be found to help get rid of or minimize the challenges to protect MANET and raise level of security in it. Several solutions have been put forward commensurate with the challenges. MANET network is expanding dynamically and evolving continuously and rapidly. With the passage of time challenges are renewed and security solutions are renewed commensurate with the developments.

REFERENCES

[1] SaloniVashisht, AnkitVashisht&Sheveta, (2014), “An Empirical Performance Evaluation of AODV and DSR using ALERT Protocol in MANET”, International Journal of Computer Applications, Vol 97.

[2] Saleh Ali K.Al-Omari , Putra Sumari, (2010), “An Overview of Mobile Ad Hoc Networks for the Existing Protocols and Applications”, International journal on applications of graph theory in wireless ad hoc networks and sensor networks,Vol2 .No 1 pp 87-110.

[3] RashmiMahajan, S. M. Patil, (2014), “A Review of MANETs Security Aspect and Challenges with Comprehensive Study of SIDS for Discovering Malicious Nodes”, International Journal of Innovative Science Engineering and Technology (IJISET), Vol. 1 Issue 6, pp241-250.

[4] T. Navaneethan, M. Lalli, (2014), “Security Attacks in Mobile Ad-hoc Networks A Literature Survey”, international Journal of Computer Science and Mobile Applications, Vol.2 Issue. 4, pp 1-7

[5] V.Umadevi, S.Geetha&G.Geetharamani, (2014),” Survey on Secure Routing Protocols in MANET”, International Journal of Advanced Research in Computer and Communication Engineering, Vol. 3, Issue 7, pp 7609-7611.

[6] CH.V. Raghavendran , G. Naga Satish& P. Suresh Varma,(2013) ,” Security Challenges and Attacks in Mobile Ad Hoc Networks”, Information Engineering and Electronic Business, vol.5, no.3,pp 49-58

[7] RashmiC.Deshmukh,BhushanN.Mahajan ,(2012),“Smart Key Management Using Incremental Grouping key Management Algorithm”, International Journal of Engineering Research and Applications (IJERA) , Vol. 2, Issue 3, pp.2607-2611.

[8] Sneha U. Agalawe ,NitinR.Chopde, (2014) “Security Issues: The Big Challenge In Manet”, International Journal of Computer Science and Mobile Computing ,Vol.3 ,Issue.3, pp. 30-34

[9] Yogendra Jain, Geetika S. Pandey&DeshrajAhirwar, (2012),” An Improved Routing Mechanism for Secure Ad-hoc Network”, International Journal of Engineering and Advanced Technology (IJEAT), Vol-1, pp 37-44.

[10] Anna Vijendran ,J.VijiGripsy, (2014) ,”A Meticulous Investigation Of Impersonation Attacks on Manets Using Different Routing Protocols”, International Journal of Computer Engineering and Applications, Volume V, Issue I, pp 106-113.

[11] RavikiranPandurangPawar, (2013), “Secure Intrusion Detection System against DDOS Attack In MANET “, International Journal of Engineering Research & Technology (IJERT), Vol- 2.

[12] Ashish M. Mishra, Charan Singh,(2014),Worm-Hole Detection Mechanism for Reactive Routing of Mobile Ad-Hoc Network, International Journal of Emerging Research in Management &Technology, Vol-3.

[13] Marwaha, S Indulska, J. &Portmann, M, (2008) ,“Challenges and Recent Advances in QoS Provisioning, Signaling, Routing and MAC protocols for MANETs”, IEEE Telecommunication Networks and Applications Conference, pp 97 – 102.

[14] S. Ahmed, A. K. Ramani, (2007) , “Exploring the Requirements for QoS in Mobile Ad Hoc Networks” Journal of Information & Communication Technology, Vol. 1, No. 2, pp 1-9.
[15] SharmilaSankar, V. Sankaranarayanan, (2010), “A Low Overhead Reachability Guaranteed Dynamic Route Discovery Mechanism for Dense MANETs”, International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC) ,Vol.1, No.3,pp 72-83.
[16] Ashwani Kumar,(2012), “Security Attacks in Manet - A Review”, International Journal of Computer Application,
[17] DharamVir, S.K, Agarwal&S.A.Imam, (2013),”Performance Analysis of MANET with Low Bandwidth Estimation”, International Journal of Scientific and Research Publications, Volume 3.
[18] Marwaha, S Indulska, J. &Portmann, M,(2008),”Challenges and Recent Advances in QoS Provisioning, Signaling, Routing and MAC protocols for MANETs”, Telecommunication Networks and Applications Conference..
[19] http://www.pcworld.com/article/2010278/10-common-mobile-security-problems-to-attack.html
[20] Ankur O. Bang, Prabhakar L. Ramteke, (2009),”MANET: History, Challenges and Applications”, International Journal of Application or Innovation in Engineering & Management (IJAIEM), Volume 2.
[21] Anuj K. Gupta, (2009),”Secure Routing Techniques for Mobile Ad Hoc Networks”, IEEE International Advance Computing Conference.
[22] KhushbooSawant, M.K Rawat,(2014),”Survey of DOS Flooding Attacks over MANET Environment”, Journal of Engineering Research and Applications, Vol. 4, pp.110-115.
[23] TusharSaxena, (2013),”Analytical Study of Attacks on Manets Based on Layered Architecture”, Cyber Times International Journal of Technology & Management, vol-6.
[24] http://www.bth.se/fou/cuppsats.nsf/all/3878ec739b12f80ac12572c2003f7d58/$file/Final_Thesis.pdf
[25] Al-Sakib Khan Pathan, (2010),”Security of Self-Organizing Networks: MANET, WSN, WMN, VANET”, 1st, pp211.
[26] Amit M Holkar, NehaShindeHolkar&DhiirajNitnawwre, (2014), “Investigation of Application Attack on MANET”, International Journal of Computer Applications, Volume 85.
[27] Athira V, Panicker, Jisha G, (2014),”Network Layer Attacks and Protection in MANETA Survey”, International Journal of Computer Science and Information Technologies, Vol. 5, NO 3.
[28] Manu Srivastava, Saurabh Mishra &Upendra Kumar Soni , Shah Fahad,(2014),” Secured 7 Layer Security Architecture (S7LSA) For Mobile AdHoc Network”, Journal of Engineering Research and Applications, Vol. 4, Issue 4, pp.01-04.
[29] Jianminchen, jiewu, (2011),”Wireless Technologies: Concepts, Methodologies, Tools and Applications”, Chapter 4.1, P864.
[30] KamanshisBiswas , Md. Liakat Ali,(2007) ,“Security Threats in Mobile Ad Hoc Network, Master Thesis, Blekinge Institute of Technology.
[31] Muhammad Arshad Ali, YasirSarwar, (2011),”Security Issues regarding MANET (Mobile Ad Hoc Networks: Challenges and Solutions”, Master Thesis Computer Science, Blekinge Institute of Technology

Author

Dr. Nabeel Mohammed Zanoon, He received his PhD in Computer Systems Engineering, from South-West State University, Kursk, Russia, in 2011. He is faculty member with Al-Balqa’ Applied University since 2011; where he is currently Assistant professor and Head of the Department of Applied Sciences as well as Director of the ICDL Computer Centre and Cisco Academy Branch of Aqaba University College. He has published several research in several areas, Security of E-Banking, Algorithm Scheduling in Grid and Cloud, Meta-Grammar, hardware and Architectural computer, Fiber optical ,Mobile Ad Hoc Networks.

Dr. Hatem S. A. Hamattareceived his B.Sc. degree in Computer Science from Yarmouk University, Irbid, Jordan, in 2003, the M.Sc. degree in Computer Science from University of Jordan, Amman, Jordan, in 2006, the PhD Degree in *Wireless Network Security* from Aligarh Muslim University, Aligarh, India, in 2014. Since 2006, he has been with the faculty of the Department of Applied Sciences at Al-Balqa` Applied University/Aqaba University College, Aqaba, Jordan; where he is currently Assistant Professor and Dean Assistant for Development and Quality Assurance. His research interests include Wireless Network Security, Mobile Ad Hoc Networks, Intrusion Detection Systems and Security Design Issues. He is also a member of the IEEE GOLD Affinity Group, Professional Communication and Computer Society. Also, he is a member of ACM and International Association of Engineers.

NashatGhalebAlbdour received his B.Sc. and M.Sc degree in Computers, Complexes, Systems and Networks from Kirovograd National Technical University, Kirovograd, Ukraine Faculty of Computer , the PhD Degree in telecommunication systems and networks from National Technical University of Ukraine, L`viv, Ukraine in 2011, He is faculty member with Department of Electrical & Computer Engineering,

Rasha M. Al-Tarawneh received her B.Sc. and M.Sc. degree in Computer Science from Al-Balqa` Applied University, Salt, Jordan, in 2008 and 2011 respectively. Since 2011, she has been with the faculty of the Department of Applied Sciences at Al-Balqa` Applied University/Aqaba University College, Aqaba, Jordan; where she is currently a full time Lecturer.