Ashraf, J Comput Eng Inf Technol 2019, 8:2
DOI: 10.4172/2324-9307.1000216

Journal of Computer Engineering & Information Technology

Review Article

A SCITECHNOL JOURNAL

Survey on the Security Issue of Mobile-Ad-hoc Network

Adeel Ashraf*

Abstract

In wired network there are lots of protections when communication occur because every node is physically connected to each other and there have minimum chance to leak the data from this wired network So, the data are safely transferred through this network. In case of wireless mobile ad-hoc network in which every node is dynamic in nature when data is transferred from one source to destination then data transfer node to nearby node and haven't centralized point. This network is established in that place where proper infrastructures are not present. Due to mobile ad-hoc network hacker have maximum chances to attack on this partial or entire wireless network. There are bundle of vulnerabilities and number of attacks are present through which data can stop for transferring to real destination and also disturbed that network. There are number of techniques are discussed in this article for preventing of data in mobile Ad-hoc network [MANNETs].

Keywords

Mobile-ad-hoc; Network; Communication; Wireless Mobile

Introduction

Through wired network data can transfer from one place to another in a very good manner. In a wired network there are re-established infrastructure are present for transfer the packets of information. The entire information packet is saved in re-designed infrastructure; they have low chances to attack on the information data path. On the other hand, wireless network through which data transfer from source to destination through nodes that is placed between sources to destination [1].

There is no re-established network infrastructure in mobile ad-hoc network. So network formed through different nodes. Every node is very necessary for transfer the packets of data. Nodes in a mobile ad-hoc network are dynamically changed from one place to other; the nodes in mobile ad-hoc network may join or leave the network due to dynamically changing of nodes from one place to other. Due to dynamic nature of mobile ad-hoc network data can loss or miss-use from network that are the security issue in changeable nodes of wireless network [2]. The nodes that can receive data then this node sent data to near node for transmission.

This mobile ad-hoc network benefits the people and organization make the network where the re-established network is not present. This mobile ad-hoc network is very easy to make. Nodes that are used in this network may be router and host or both [3].

***Corresponding author:** Adeel Ashraf, School of Computing, Engineering and Intelligent Systems, Magee campus, Ulster University, Coleraine, Northern Ireland, Tel: 3137388266; E-mail: adeelashraf593@gmail.com

Received: January 22, 2019 **Accepted:** February 04, 2019 **Published:** February 11, 2019

Mobile ad-hoc network works without re-established infrastructure (Figure 1). This network face lots of security issue challenges that are data consumption, Quality of services, bandwidth utilization due to distributed and dynamic changing of MANNETs nodes [4]. This type of security issue can be solved through different techniques in mobile ad-hoc network.

Data can transfer through dynamic nature in certified authentication handshake process, cryptography and firewall [5]. When dynamic nature nodes going to hostile environment with poor protection then this type of node may launch attacked in ad-hoc network [6]. So authentication, encryption or firewall techniques can be used for data saving in mobile ad-hoc network.

Related work

In the mobile ad-hoc network there are so many research paper were concluded for the best choice of security issue of mobile ad-hoc network. Lot of problem present in the security issue of MANNET's like data are transfer from source to destination through dynamic nodes, so in this case data packet can be disturbed and the data may be hacked by different opponents each nodes is compulsory for the transfer of data that is basic issue for mobile ad-hoc network. In this security issue survey and research have done for the secure of wireless data [7].

The optimal path is basic challenge for transfer of data, in this issue solutions are purposes for best optimal path for data that is for route selection for combining ad-hoc on demand distance vector (AODV) protocol with ant colony organization to improve the quality of service.

In this process that have very suitable techniques for data transformation by combining the router. The algorithm used for this demand lengthy protocol helpful for data security that are Dynamic Source Routing (DSR) that are not used for dynamic router [8].

Through this protocol route will be selected for data transmission that is very important for data security of data transmission, no one

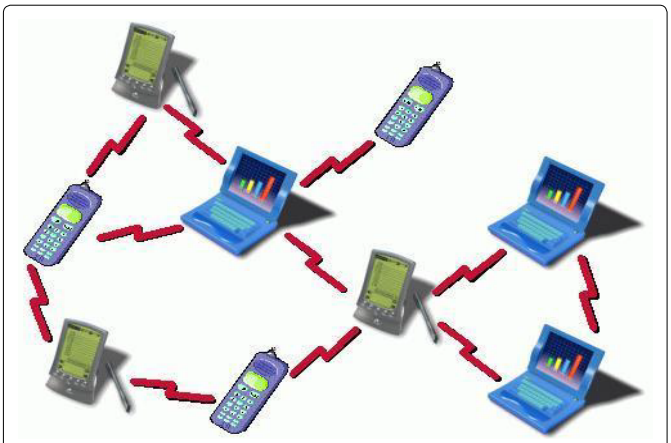

Figure 1: Structure of mobile ad-hoc network [33].

Note: These mobile ad-hoc networks are used in following field [3]:

Military Battlefield, Sensor Networks, Commercial Sector, Medical Service, Personal Area Network.

can hack the data that is used in military task and other framework where re-establish infrastructure are not present [9].

When data is transferred from source to destination through different nodes then security issue of data transfer is present so for this security issue lots of surveys and research papers were written for the conclusion of this data hacking and data disturbing [10].

In the previous paper to solve the problem method is used for encrypt the data that is used for secure for significant data transfer in this case data that is transfer form source side then firstly data is encrypted when data is transfer through node to node if anyone wants to get the data that is difficult for that person because data is encrypted through specific algorithm. Data is securely transferred from one end to the destination in the best way manner, the method that are familiar to encryption are SSDE and toss-a-Coin method for data security issue [11].

When data is transferred from one end to destination side then lots of hurdles are present in this areas but this type wireless mobile ad-hoc network can be run in very easy way where there are no re-establish infrastructure like military side, battle field, desert side nothing can reach that border type place so in this network data is transferred through nodes. Node may vary through different type like mobile, vehicle and other device [12]. Data is transferred during quickly situation and next action performed depend on this data come on this network. In this network there are many difficulties for data transfer, so many techniques for avoid the difficulties one techniques that is used for the survey of data transferred. For data transfer rising demands are cellular network needs to suitable changes (Table 1) [13] for cellular network device-to-device communication are establish for data transfer in secure easy way. Architecture also proposed for the implementation of device to device communication this device-to-device communication (D2D) is mainly focus on the security issue of the mobile ad-hoc network [14].

Another survey that are used for data secured and mainly stared on the security issue of the wireless mobile ad-hoc network. In this survey main techniques for the security of issue of data transfer from one end to the other are Opportunistic Networks, through this network you can save your data security and data are easily send through this network [15].

This type of network proposes unifies framework for implementation of this Opportunistic network that Is mainly focused on issue of data that is transferred from one place to other place [16].

Data transfer through mobile nodes with service without fixed infrastructure that are mainly focused for the security attack. Nodes are like router that carries information from one place to other [15].

The techniques used for secured data transfer are very interesting this technique follow the cloud based that are used for mobile ad-hoc network. Firstly, we describe the threats and propose security services for this techniques [17].

Wireless mobile ad-hoc network framed without re-establish infrastructure with no central entity for the transfer of data that are self-governing arrangements in this research survey he present a most promising effective techniques to defend wireless ad-hoc network. Energy system based system for the data transfer from source to destination. We discuss the challenging research issue and for mitigating the Sybil attack in wireless ad-hoc network [18].

These mobile ad-hoc networks are very flexible network that are very easy to make in the border of any two countries where re-established infra-structure are not present, information transfer from node to node. The nodes are dynamic in nature transfer data dependent on neighbor nodes to reach on destination place. in this research paper you can use QASEC to achieve the better throughputs by securing end-to-end communication in mobile ad-hoc network. Our proposed QASEC scheme prevents the malicious nodes from

Table 1: Comparison of different Article of Mobile Ad-hoc Network.

Reference No.	Paper Tittle	Author Name	Description
[25]	Multilevel security model for ad hoc networks	Wang Changda and Ju Shiguang	Mobile Ad-hoc network are establish in that place where no infrastructure is present in this article search on secure routing level and computing powers for better security. It have-different security level that are controlling restricted classified information flows among nodes
[26]	RKP based secure tracking in wireless sensor networks	Wang Jiahao, Qin Zhiguang, Geng Ji and Wang Shengkun	To enhancing security of mobile Ad-hoc Network. This article proposes a tracking cluster based mobile cluster distributed group rekeying protocol (MCDGR). Cluster follow the target nodes and process that data for security
[27]	Enhancing secure routing in Mobile Ad Hoc Networks using a Dynamic Bayesian Signalling Game model	M Kaliappan, B Paramasivan	It is very essential to secure the nodes for protecting the data. In his article Game theory is currently employed to analysis the malicious node for protecting data
[28]	NMA in MANNET's using combining Algorithm	MSS Khan, Anupum Kamar, Bin Xaid, and Prasona K.	Due to lack of centralized node there have no security of data between node to node. In this article techniques are used for securing the data are EM, MLE, stitching algorithm for better security of data in wireless network.
[29]	A Prevention System against fully Attacks in Mobile Ad hoc Networks	Farrukh Alam Khan, Muhammad Imran, Haider Abbas, Muhammad Hanif Durad	There are number of attacks occour on wireless ad-hoc network. The techniques for securing data are special node like DPS find that node that have suspicious behavior secure the data of the nodes
[30]	Data packet collect for error detection in MANNET's;A survey	Gaong Liua, Zeng Yana, Vitald Pedryczc,	In mobile ad-hoc network various attacks occurs on data node, the technique used for data securing are intrusion detection and Data Collection for securing data that are very important for securing data
[31]	Performance of PKI-based security mechanisms in mobile ad hoc networks	Christian Schwingenschlögla, Stephan Eichlerb, Bernd Müller-Rathgeberb	Security for ad hoc network receive lot of techniques for secure your nodes of data that are focusing on secure routing, fairness issues and malicious node detection. In this article the main techniques are PKI technology and LKN-ad hoc security for secure data
[32]	Security and trust issues in Fog computing: A survey	PeiYun Zhang, MengChu Zhou, Giancarlo Fortino	In this network due to lack of central point there no security of data when your nodes move from one place to other so the techniques use for securing data are quality of service QoS make the distance of changeable node in quality measurement

data exchange with legitimate intermediate nodes on any established path between the source and the destination [19].

Lot of research paper defined lot of scheme for the security information for transfer from node-to-node. In this research paper technique used for securing data are heretical routing protocol for secure transfer of information from source to destination [20]. Prevention of security attack in data that is transferred from one place to another place for well-known purposes. The technique that is used for transfer of data is TGNDCS to verify the wireless network security protocol. In this technique researcher use TGNDCS to perform security analysis of three well known wireless sensor network [21].

Mobile ad-hoc network that are establish on that place where infrastructure is not present, in the deserts, battle field of two armies, this wireless network is also used in the war place for patient bring to hospital data is transferred from one node to other node, the node may be ambulance, router, other device used for transmission of information [22].

In this mobile ad-hoc network main factor are the security issue that effect importantly on the whole network that wireless network sometimes establishes for intelligent operation and become a security issue on this network, the techniques used to control the security threats of this wireless network. The purpose of this techniques is used to converging the sensory network into MANNETs network because the nodes have different power level for the transmission of data and secure the data from illegal work [23].

Service oriented architecture(SOA) for the purpose of data security that is an evolution of past platform for the best services of data security for maintenance of the data work in the issue of data that type of network are establish where re-establish infrastructure are not present [24-32].

Conclusion

In this paper authors have fully tried to discuss all the problems that occur in the wireless mobile ad-hoc network and also elaborate the preventing techniques through which data can safe when move from source to destination through dynamic nodes. When you are study mobile ad-hoc network then lots of vulnerability have in your mind and security issue face in this wireless network. All the discussion in this paper are very understandable and beneficial to avoid the problem and use the techniques through which data can safely transferred from node to node in the absence of central node. Authors are fully confident to discuss the method and their expertise with better system and enhanced features in mobile ad-hoc network MANNETs.

References

1. Al-Janazi S, Al-Shourpaji I, Shozafar M, Shamshairb S (2016) Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications Egyption. Informations J 18: 112-122.
2. Navaneethan C, Meenatchi S, Mutyala VSR, Thamaraiselvi V (2015) An optimistic approach for data retrieval in vehicular adhoc networks. Procedia Comput Sci 50: 380-387.
3. Kaur N, Kad S (2016) A review on security related aspects in vehicular adhoc networks. Phys Procedia 78: 387-394.
4. Bahry FDS, Anwar N, Amran N, Rias RPM (2015) Conceptualizing security measures on mobile learning for Malaysian higher education institutions. Procedia Soc Behav Sci 176: 1083-1088.
5. Li W, Joshi A (2008) Security issues in mobile ad hoc networks: A survey. Dep Comput Sci Electr 92: 1-23.
6. Salama A, Saatchi R (2018) Probabilistic classification of quality of service in wireless computer networks. ICT Express 1-8.
7. Ahmad M, Ikram AA, Wahid I, Inam M, Ayub N, et al. (2018) A bio-inspired clustering scheme in wireless sensor networks: BeeWSN. Procedia Comput Sci 130: 206-213.
8. Sarkar D, Choudhury S, Majumder A (2018) Enhanced-Ant-AODV for optimal route selection in mobile ad-hoc network. J King Saud Univ Comput Inf Sci 2018.
9. Omar M, Boufaghes H, Mammeri L, Taalba A, Tari A (2016) Secure and reliable certificate chains recovery protocol for mobile ad hoc networks. J Netw Comput Appl 62: 153-162.
10. Bhalaji N, Shanmugam A (2012) Dynamic trust based method to mitigate greyhole attack in mobile adhoc networks. Procedia Eng 30: 881-888.
11. Kushwaha A, Sharma HR, Ambhaikar A (2016) A novel selective encryption method for securing text over mobile ad hoc network. Procedia Comput Sci 79: 16-23.
12. Dhivya P, Karthik S, Kalaikumaran T (2014) MTOM technique for secure data transmission over CMEA protocol in MANET. Int J Appl Eng Res 9: 4809-4812.
13. Li C, Zhu L, Tang H, Luo Y (2018) Mobile user behavior based topology formation and optimization in ad hoc mobile cloud. J Syst Softw.
14. Gandotra P, Jha RK, Jain S (2017) A survey on device-to-device (D2D) communication: Architecture and security issues. J Netw Comput Appl 78: 9-29.
15. Sabu ES, Nakarazu S, Prasad MSNO (2015) Analysis of secure routing protocol for wireless adhoc networks using efficient DNA based cryptographic mechanism. Procedia Comput Sci 70: 341-347.
16. Zakhary S, Benslimane A (2017) On location-privacy in opportunistic mobile networks, a survey. Netwz Cozmput Apple 102: 157-170.
17. Sharma G, Bala S, Verma AK (2012) Security frameworks for wireless sensor networks-review. Procedia Technol 6: 978-987.
18. Vasudeva A, Sood M (2018) Survey on sybil attack defense mechanisms in wireless ad hoc networks. J Netw Comput Appl 120: 78-118.
19. Usman M, Jan MA, He X, Nanda P (2018) QASEC: A secured data communication scheme for mobile Ad-hoc networks. Futur Gener Comput Syst.
20. Varshney S, Kumar C, Swaroop A (2018) Leach based hierarchical routing protocol for monitoring of over-ground pipelines using linear wireless sensor networks. Procedia Comput Sci 125: 208-214.
21. Macedonio D, Merro M (2014) A semantic analysis of key management protocols for wireless sensor networks. Sci Comput Program 81: 53-78.
22. Yoshida N (2006) Type-based security for mobile computing integrity, secrecy and liveness. Electron Notes Theor Comput Sci 162: 333-340.
23. Mukherjee S, Biswas GP (2018) Networking for IoT and applications using existing communication technology Egypt. Informatics J 19: 107-127.
24. Farkhana M, Hanan MAA (2018) Mobility in mobile ad-hoc network testbed using robot: Technical and critical review. Rob Auton Syst 108: 153-178.

25. Changda W, Shiguang J (2008) Multilevel security model for ad hoc networks. J Syst Eng Electron 19: 391-397.

26. Jiahao W, Zhiguang Q, Ji G, Shengkun W (2008) RKP based secure tracking in wireless sensor networks. J Syst Eng Electron 19: 175-183.

27. Kaliappan M, Paramasivan B, Rehmani M (2015) Enhancing secure routing in Mobile Ad Hoc Networks using a dynamic bayesian signalling game model. Comput Electr Eng 41: 301-313.

28. Khan MAH, Kunnar A, Xieng A, Rannar PM (2015) Network tomography application in mobile ad-hoc network using stitching algorithm. J Netw Comput Appl 56: 77-87.

29. Khan FA, Imran M, Abbas H, Durad MH (2017) A detection and prevention system against collaborative attacks in mobile Ad hoc networks. Futur Gener Comput Syst 68: 416-427.

30. Liu G, Yan Z, Pedrycz W (2018) Data collection for attack detection and security measurement in mobile ad hoc networks: A survey. J Netw Comput Appl 105: 105-122.

31. Schwingenschlögl C, Eichler S, Müller-Rathgeber B (2006) Performance of PKI-based security mechanisms in mobile ad hoc networks. Int J Electron Commun 60: 20-24.

32. Zhang PY, Zhou MC, Fortino G (2018) Security and trust issues in fog computing: A survey. Futur Gener Comput Syst 88: 16-27.

Author Affiliation

Top

School of Computing, Engineering and Intelligent Systems, Magee campus, Ulster University, Coleraine, Northern Ireland