International Journal of Research and Review
www.ijrrjournal.com E-ISSN: 2349-9788; P-ISSN: 2454-2237

Review Article

A Review of Communication and Data Attacks in Mobile Network

Rekha[1], Radhika Garg[2]

[1]Student, M.Tech. (CSE), Vaish College of Engineering, MDU, Rohtak
[2]Asstt. Prof., CSE Dept., Vaish College of Engineering, MDU, Rohtak

Corresponding Author: Rekha

ABSTRACT

A Mobile network is the open network which is available globally to all public and private users. The generally cannot be restricted to enter in this network. Because of this, the network suffers from various kinds of security challenges. The internal and external communication attacks can results the communication loss or the data theft. In this paper, a study on different kind of communication and data attacks is provided. These attacks are generated by generating the fake entities, fake packet or the fake control message communication. The paper has explored the security challenges in the mobile network and identified some of the common data centric network attacks.

Keywords: Mobile Network, Network Security, Data Attacks, Communication Loss.

1. INTRODUCTION

A mobile network is one of the most common and busiest networks which provide the interconnection between mobile nodes in the public domain. The wires communication and the resource sharing is possible using the mobile network. The network does not require any centralized controller to perform the transmission between the nodes. When the communication between two nodes is performed, lot of other nodes act as the intermediate nodes. The network communication and route optimization can be applied in this network form to optimize the communication strength. The basic structure of mobile network is shown in figure 1.

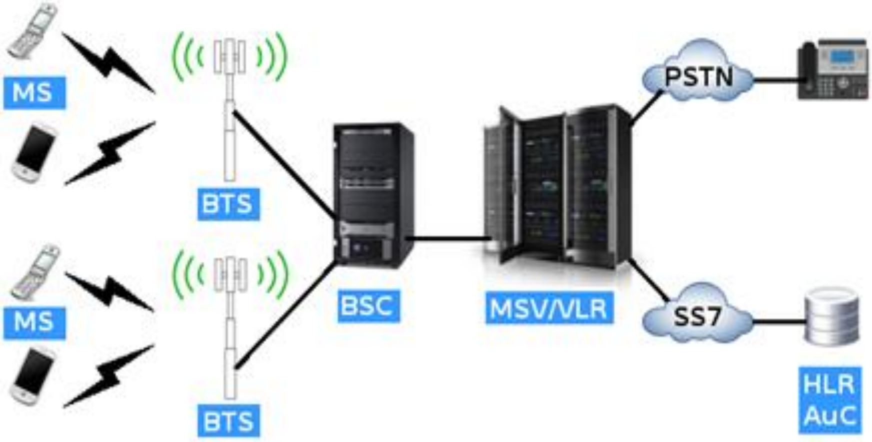

Figure 1 : Basic Structure and Component of Mobile Network

Here figure 1 is showing the structural, functional and the component driven architecture for mobile network. The mobile stations are the mobile devices present at the lowest level and perform the communication. In the region, the mobile devices can communication directly. To provide the service sharing and the signal distribution, the BTS stations are established with coverage specification. Each mobile station is covered by the BTS. The BTS is responsible to track the mobile nodes and to provide the distribution of various voice and data services. The authority and the control to these BTS is provided by BSC specific to the regional coverage. The BSC is further connected to the MSV for connection to other networks. The figure is showing the connectivity to the other network forms.

From this figure, it is observed that the mobile network is the vast network form that provides the sharing or communication between the mobile devices. This vast communication scope in the network also open up the network to the various kind of network attacks. The network suffers from different kind of attacks. These common attack forms and relative solutions are shown in figure 2.

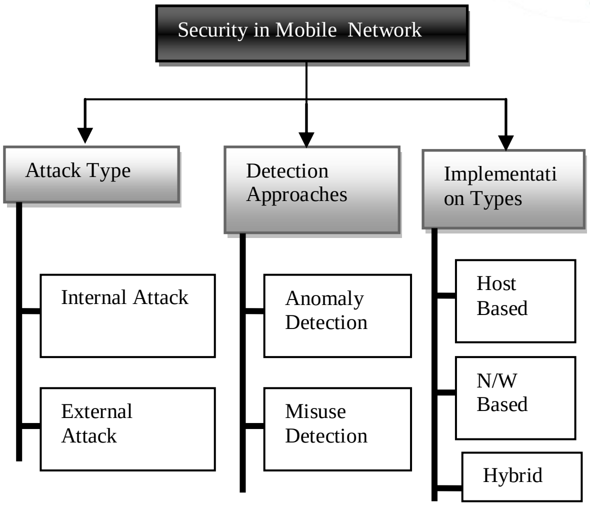

Figure 2: Security in Mobile Network

Here figure 2 is showing the security driven aspects relative to the mobile network. The figure showing the tree main constraints called attack type, detection methods and the implementation methods. The figure shows that the network suffers from two types of attacks called internal and external attacks. To perform the detection of these attacks, various attack behavior analysis methods are defined. These methods include Anomaly detection and misuse detection in mobile network. The implementation of these attack detection methods can be done either on individual node or network or the combination of both. In this paper, an exploration to different kind of attacks in the mobile network are provided and discussed. The work already provided on the study and detection of different attack is provided in section II.

2. EXISTING WORK

A mobile network suffers from different kind of network attacks. These attacks can increase the information loss and break the network communication. In this section, the work provided by earlier researchers is discussed. Author [1] has defined a global model to analyze the different traffic driven problems in the network. The data mining method is defined to evaluate the risk factors and the criticality of communication risk. The method is defined to recognize the DOS attack in the network and the method to reduce the impact of this network attack. Author [2] has defined a work on energy level assessment to the network and identify the work in terms of architectural configuration. The control message specific attacks that increase the communication loss are discussed in this paper. The energy loss analysis and the attack identification is provided in this work. The evaluation of communication loss at different levels is provided in this work. Author [3] has defined a study work to detect the intrusion over the public network and to provide the safe communication. The response based evaluation parameters and the intrusion detection methods and measures are defined by the author. The feature level estimation was provided to improve the network reliability and to reduce the communication loss. Author [4] has presented the probabilistic model is defined to detect the attack and to generate the safe communication over the network. The frequency driven analysis was provided by the author based on the frequency level analysis. The attack identification and the network improvement in the defensive method to identify the misbehavior of nodes. The frequency measure was defined to observe the network traffic and to generate the safe communication. Author [5] has defined a work on the pattern based analysis to generate the effective communication in the physical environment. The activity specific security method was defined to improve the communication reliability. The authentication driven analysis was provided to analyze the network reliability. The conditional analysis was provided to reduce the intrusion detection. Author [6] has defined a work on the attack defensive communication method to detect the attack and to generate the safe communication. The attack detection and reduction method is provided in this work.

Author [7] has provided an attack detection approach based on the pattern mining on the communication behaviour of the network. The dictionary specific attack analysis method was defined to analyze the communicating information over the network. A substantial feature analysis was provided to detect the network against different attacks. Author [8] has defined a hybrid system based on the communication parameter evaluation at different network layers. The random field based violation analysis was defined to improve the communication behavior in the network. Author [9] has defined a statistical method to detect the misbehavior and to generate the preventive route formation in the network. The traffic learning method was defined to detect the attack and the suspicious activity over the network. The attack detection and prevention was provided by the author to improve the network communication. Author [10] has defined a statistical realistic method to improve the communication against the test data. The algorithmic method is defined to detect the intrusion in the mobile network. The realistic data processing was provided by the author for attack detection and prevention in the network.

Author [11] has defined a work on Poisson process model analyze the network and to improve the network communication. The markov model is defined with probabilistic measures to detect the attack and to provide the safe communication against the attack. The alert system is defined to generate the safe communication and to increase the network security. Author [12] has used the clustering based method for similarity based analysis on the network attacks. The statistical observations was provided and considered to detect the abnormal communicating activities in the network. Author [13] has defined a realistic method to detect the error for attack detection in the mobile network. The communication feature observation and the packet communication was provided for the network. Author [14] defined a work on the pattern analysis for web based system. The observation on the communication structure was provided to detect the attack and to improve the network communication. Author [15] has defined a parametric approach to process the application specific statistics to detect the attack and to generate the safe communication over the network. The structure specific safe communication was provided by the author.

3. VARIOUS ATTACKS IN MOBILE NETWORK

The mobile network is completely open network in the public domain that increases the security challenges for this network type. The network suffers from different kind of communication and data centric attacks. The functionality is defined to detect the communication pattern and to detect the safe and unsafe communication. The control analysis is provided to detect the different kind of network attacks. The common attacks in this network are listed below

A) Spoofed, Altered, or Replayed Routing Attack

This kind of network attack is performed on the intermediate nodes of the communication route. The attack is identified in terms of loops, disruption, false message generation, route diversion, delay increase etc. These kind of attack is defined to modify the identity of the intermediate node because of this, the path length increased and the communication delay occur. The repetition of a node in the path is done to move the packets in a close tunnel and the communication is performed continuously between two intermediate nodes as a loop.

B) Selective Forwarding

The functioning of mobile network is to generate the dynamic path. The path formation is done by selecting the effective next forwarding path. The analysis on the forwarding path can be done based on the communication level evaluation. The packet level analysis and prop evaluation was applied on each node and the effective node is selected. The blackhole is one such attack that captures the communication and refuses the data forwarding. The data flow evaluation is required to generate the safe communication against these attacks.

C) Sinkhole Attacks

The sinkhole attack is another identity morphing attack in which the intermediate node or the network node represents itself as the fake identity. The node affects the quality of the node communication and avoids the data delivery to the network node. The neighbor node analysis is done to identify the compromise the network node. The route formation and the node necessarily evaluation was provided to generate the safe communication over the network. The sinkhole attack increases the communication loss over the network.

D) Sybil Attack

In this network form, the multiple identities are generated on the network nodes to capture the network communication and to increase the communication fault. The fault can be generated at node level and network level so that the disruption can be generated over the network. The routing protocol is defined to generate the safe communication over the network.

E) Rational Attack

The rational attack is another cooperative attack that disrupts the communicating information so that the communication loss can occur over the network. The resource level analysis is done to increase the load over the available resources and instances and the communication loss can increase during the communication.

4. CONCLUSION

In this paper, an exploration to the different kind of network attacks is provided. The mobile network is the open network form defined with mobile network and communication behavior. The defensive mechanism is defined to control the data packets and that affect the network. The common attack types and their work behavior is also described in this paper.

REFERENCES

1. Rishabh Jain, Charul Dewan, Meenakshi, *A Survey on Protocols & Attacks in MANET Routing*, IJCSMS International Journal of Computer Science & Management Studies, Vol. 12, Issue 03, September 2012 ISSN (Online): 2231 –5268
2. Pramod Kumar Singh, Govind Sharma, *An Efficient Prevention of Black Hole Problem in AODV Routing Protocol in MANET*, 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications.
3. Wazir Zada Khana, Yang Xiangb, Mohammed Y Aalsalema, Quratulain Arshada *"The Selective Forwarding Attack in Sensor Networks: Detections and Countermeasures",* I.J. Wireless

and Microwave Technologies, 2012, 2, 33-44 Published Online April 2012 in MECS.

4. Sudhir Agrawal, Sanjeev Jain, Sanjeev Sharma, *A Survey of Routing Attacks and Security Measures in Mobile Ad-Hoc Networks*, Journal Of Computing, Volume 3, Issue 1, January 2011, ISSN 2151-9617.
5. Y. C Hu, A. Perrig and D. Johnson, "Wormhole Attack in Wireless Networks," IEEE JSAC, vol. 24, no. 2, Feb. 2006.
6. H.S. Chiu and K.S. Lui, “DelPHI: Wormhole Detection Mechanism for Ad Hoc Wireless Networks,” in Proc. International Symposium on Wireless Pervasive computing, Phuket, Thailand, pp. 1-6, 2006.
7. I. Khalil, S. Bagchi, N.B. shroft "LiteWorp: Detection and isolation of the wormhole in static mulihop wireless network. Journal," Acm: The international Journal of Computer and Telecommunications Networking Archive, Vol. 51, Issue 13, September 2007.
8. Ritesh Maheshwari, Jie Gao and Samir R Das “Detecting Wormhole Attacks in Wireless Networks Using Connectivity Information” INFOCOM.1-4244-1047-9 IEEE May.2007.
9. Marianne A. Azer, Sherif M. El-Kassas, Abdel Wahab F. Hassan, Magdy S. El-Soudani “Intrusion Detection for Wormhole Attacks in Ad hoc Networks a Survey and a Proposed Decentralized Scheme” IEEE DOI 10.1109/ ARES.2008.177
10. Sun Choi, Doo-Young Kim, Do-hyeon Lee, Jae-il Jung "WAP: Wormhole Attack Prevention Algorithm in Mobile Ad Hoc Networks" 2008 IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing.
11. Saurabh Gupta Subrat Kar S Dharmaraja, “WHOP: Intrusion Detection Protocol using Hound Packet”, 2011 International Conference on Innovations in Information Technology.
12. Pallavi Sharma Prof. Aditya Trivedi, “An Approach to Defend Against Intrusion in Ad Hoc Network Using Digital Signature”, 978-1-61284-486-2 IEEE.
13. Tarek Sheltami and Hussein Mouftah “Comparative study of on demand and Cluster Based Routing protocols in MANETs”, IEEE conference, pp. 291-295, 2003.
14. B.J. David, “The dynamic source routing protocol for mobile ad hoc networks (dsr)”, Internet-Draft, 2004.
15. C.E. Perkins, E.M. Royer, “Ad-hoc on-demand distance vector routing”, In, IEEE WMCSA 99, pages 90 –100, feb 1999.

How to cite this article: Rekha, Garg R. A review of communication and data attacks in mobile network. International Journal of Research and Review. 2017; 4(8):34-38.

******