Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 3, March 2015, pg.21 – 26

RESEARCH ARTICLE

Attacks in Opportunistic Networks

Mandeep Kaur

Doaba Institute of Engineering and Technology, Kharar

Abstract: MANET is an infrastructure based network in which nodes can be moved easily. It has one sub category also known as opportunistic network networks. All nodes are work on store and carry scheme in it. This network has some security issues. Malicious node can easily trigger attacks on this network. In this paper we will be discussed about various types of attack in an opportunistic network. The main problem which is faced in this network will also be discussed.

Keywords: MANET, Active, Passive, Attacks and store-carry scheme.

1. Introduction

Mobile Ad hoc Networks is one of type of nodes in MANETs are mobile, so they can change their location to their requirements. They may enter to a network, leave a network and also can switch on/off their connectivity. Hence no fixed infrastructure is present in this network. Nodes are connected wirelessly and also responsible for data forwarding .Nodes can also track the topology of the network to forward the message packets [1]. Due to mobility and the activation or deactivation of nodes topology may change, so all nodes also share the routing information and keep track of this. Power consumption of node is also making change in topology of network. An opportunistic network is one of the type of network [2]. An opportunistic network is a class of delay tolerance network. It is formed by the nodes having capability to support this network, the nodes are connected wirelessly [5]. The nodes are mobile or stable so no fixed

infrastructure is present in this network and this network can work even in disconnected environment. Every node have a finite range in which the can communicate or can forward the message. A node can forward a message only when any other node comes in his range. The nodes have to store the massage until another node is not come in his range. All nodes have to work in the store-carry-forward manner in this network. In this network, group of intermediate nodes help to send a message from source to destination [6]. Nodes have no predefine topology of the network, two node might be or never connected, no fix route between two node is use to send message. Network topology may change due to activation and deactivation of the node. If destination node is not in the range of source node then it passes the message to the nearest node in its range and so on node by node closer to the destination.

This network is very easy to implement in any situation or any environment like war and disaster prone areas where communication is for short time and needs very quickly. In such environment have less time to implement the network topology or to make an infrastructure [5]. At such a location or time this network is very useful to facilitate the user to communicate.

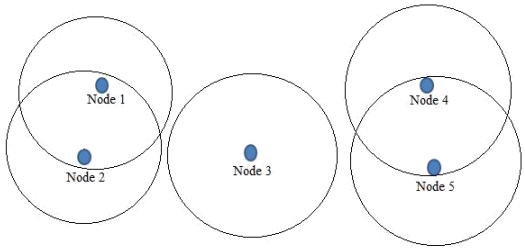

Fig 1.1 Opportunistic network

Message is passes through many nodes and these nodes are simply the devices which support this network, so there is a chance that the node is malicious once [4], now there is a problem to authenticate the nodes and may threat to the privacy of the users of this network. Many users doesn't want to disclose their identity to all the nodes of the network, due to this many user step back from this network. Node 3 does not aware of the existence of node1, node2, node4 and node5 because they are not in the range of node 3.Node 1 and Node2 is known to each other, as they are in the range of each other, but Node3, Node4 and Node5 is invisible for them, and the same thing is apply for node4 and node5. Node1 and Node2 can communicate.Node4 and Node5 can communicate.

2. Review of Literature

Carlos O. Represented [1] opportunistic Networks are able to exploit social behavior to create connectivity opportunities. This paradigm uses pair-wise contacts for routing messages between nodes. In this context they investigated if the "six degrees of separation" conjecture of small world networks can be used as a basis to route messages in Opportunistic Networks. They propose a simple approach for routing that outperforms some popular protocols in simulations that are carried out with real world traces using ONE simulator. They conclude that static graph models are not suitable for underlay routing approaches in highly dynamic networks like Opportunistic Networks without taking account of temporal factors such as time, duration and frequency of previous encounters. **G. Costantino** found [2] that message forwarding is a fundamental brick to spread information among users in opportunistic networks. In this report, they consider the recently proposed interest-casting networking primitive for opportunistic networks, in this a packet generated by a sender should be delivered to all users in the network -potentially unknown to the sender same interest in that. However, the implementation which is used now is of interest-casting assume from users to make forward decision they have to exchange their interest profile, which is very sensitive information of user and not forward to strangers, that's why they mention a technique and proposes an easy way of message sharing between users interested in same subject or topic. However, it is implicitly based on a fully trusted network, even if a malicious node can be completely trusted. In this work, they approach for the first time the problem of designing an interest-casting protocol while not revealing sensitive information during the forwarding and message delivery process. They also present a privacy hiding mechanism based on the well-known persons like business persons problem allowing users to discover whether they have similar interests without showing their private information. **Anshul verma** introduce [3] a new integrated routing protocol for opportunistic network. Existence of a fixed path is between sender and receiver not possible in opportunistic network. Information about the context in which the user communicates is a key piece to design an efficient routing protocol for this network. In this article the focus on the context information about the user to form an efficient routing protocol. They found that if a user is very isolate then context information can't be distributed, and not able to take efficient routing decision. **Xingguang Xie** found routing [4] as a big challenge in opportunistic network and proposes a social relationship predictable protocol. In this protocol they assume that the user of opportunistic network only visits some predefined places which is

preferable by the user. In this paper the combine two protocols social attribute of node mobility of social network and prediction base routing to propose social relationship enhanced protocol in opportunistic network (SREP). This will help to improve the opportunistic networks delivery ratio.

3. Attacks in Opportunistic Network

There are a variety of attacks possible in MANET. The attacks can be classified as active or passive attacks, internal or external attacks, or different attacks classified on the basis of different protocols [7] [8]. A passive attack does not disrupt the normal operation of the network. The attacker only snoops the data exchanged in the network without altering it. It includes Eavesdropping, jamming and traffic analysis and monitoring. In case of active attacks, the attacker attempts to alter or destroy the data being exchanged in the network. This attack disrupts the normal functioning of the network [9]. Active attacks can be internal or external. External attacks are carried out by nodes that do not belong to the network. Internal attacks are from compromised nodes that are part of the network. Since the attacker is already part of the network, internal attacks are more severe and hard to detect than external attacks .The ultimate goals of the security solutions for MANETs is to provide security services, such as authentication, confidentiality, integrity, authentication, non-repudiation, and availability to mobile users. The various possible attacks are:

Black hole attack, In this attack, an attacker uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. When the attacker receives a request for a route to the destination node, it creates a reply message which advertises itself as a valid path to destination. The attacker consumes the intercepted packets without any forwarding [10]. **Gray hole Attack** is also termed as misbehaving attack. In this attack, the attacker selectively drops the packet with certain probability. Also, in this attack the intruder node behaves maliciously for the time it selectively drops the packets and then switches to its normal behavior. **Wormhole attack [11]** an attacker records the packets at one location in the network and tunnels them to another location. The routing can be disrupted when routing control messages are tunneled [6]. This tunnel between two colluding attackers is referred as a wormhole. **Selective Packet Drop** is a packet dropping attack is launched on the forward phase [11]. So it is very complex and difficult to isolate. This attack is very easy to perform but very

difficult to detect it. Selfish node also drop packet in their different ways. They drop packets only to save their resources not damage any other nodes. Selective forwarding attacks may damage some mission of applications.

4. Problem Formulation

The aim of the implementing privacy in the opportunistic network is to attract more users to use this network. As privacy is the main concern and in this network there is not a fixed infrastructure is present and the message is forward through many intermediate nodes, there may be a selfish node which is not interesting to forward the message to a particular destination, or the user doesn't want to show his identity when want to communicate or send message to a particular destination, then it is risk to the privacy of user or the packet dropped by the selfish node. Also the content of message is also access by the intermediate nodes, so there is a problem that how to encrypt the message and share a key between source and destination without showing it to intermediate nodes. To overcome this problem, new technique will be proposed so that attack can be detected and isolate from the network.

5. Conclusion

An opportunistic network is a class of delay tolerance network. It is formed by the nodes having capability to support this network, the nodes are connected wirelessly. The nodes are mobile or stable so no fixed infrastructure is present in this network and this network can work even in disconnected environment. Every node have a finite range in which the can communicate or can forward the message. Various types of attacks can be triggered by the malicious node in the network. This paper concluded that opportunistic network has security issue. The attack was triggered by the malicious node which decreases the performance of the network. So a novel technique will be proposed to overcome this problem.

References

[1] Daru Pan Zhaohua Ruan Nian Zhou Xiong Lin and Zhaohui Song, "A comprehensive-integrated buffer management strategy for opportunistic networks", EURASIP Journal on Wireless Communications and Networking, 2013

[2] Carlos O. Rolim Valderi R. Q. Leithardt, Anubis G. Rossett Tatiana, F. M. dos Santos Adriano M. Souza Cláudio F. R. Geyer, "Six Degree of separation to improve routing in opportunistic networks", International Journal of UbiComp (IJU), Vol.4, No.3, July 2013

[3] G. F. Martinelli, P. Santi, "Privacy-preserving interest-casting in opportunistic networks" IEEE wireless communications and networking conference: mobile and wireless networks. WCNC 2012: 2829-2834

[4] PAPAJ Jan, DOBOS Eubomir, CUMAR, " Opportunistic Networks and Security" Journal of Electrical and Electronics Engineering, Volume 5, Number 1, May 2012

[5] L. Lilien, Z. H. Kamal, V. Bhuse, and A. Gupta, The Concept of Opportunistic Network and their Research Challenges in Privacy and Security, Mobile and Wireless Network Security and Privacy, Book Chapter, pp. 85-117, 2006.
[6] L. Pelusi, A. Passarella, and M. Conti, "Opportunistic Networking: data forwarding in disconnected mobile ad hoc networks," IEEE Communications Magazine, vol. 44, no. 11, Nov. 2006
[7] Priyanka Goyal, Vintra Parmar and Rahul Rishi , " MANET: Vulnerabilities, Challenges, Attacks, Application" , *IJCEM International Journal of Computational Engineering & Management*, Vol. 11, January 2011 ISSN (Online): 2230-7893 2011
[8] S. Sharmila and G. Umamaheswari, " Defensive Mechanism of Selective Packet Forward Attack in Wireless Sensor Networks", *International Journal of Computer Applications (0975 – 8887) Volume 39– No.4, February 2012*.
[9] LathaTamilselvan and V Sankarnarayana, " Prevention of Black Hole Attack in MANET", Journal of Networks, Volume 3, Number 5, 2008, pp 13-20.
[10] S.Marti, T.J.Giuli, K.lai and M.bakery "Mitigating routing misbehaviour in mobile ad hoc networks", 6th MobiCom, Boston, Massachusetts, August 2000.
[11] Caimu Tang ,Dapeng Oilver "An Efficient Mobile Authentication Scheme for Wireless Networks",*IEEE,* 2011
[12] N.Bhalaji and Dr.A.Shanmugam, "Reliable Routing against Selective Packet Drop Attack in DSR based MANET", JOURNAL OF SOFTWARE, VOL. 4, NO. 6, AUGUST 2009
[13] Rusha Nandy, "Study of Various Attacks in MANET and Elaborative Discussion Of Rushing Attack on DSR with clustering scheme" *International Journal of Advanced Networking and Applications Volume: 03, Issue: 01, Pages:1035-1043, 2011*

