International Journal of Engineering Research-Online
A Peer Reviewed International Journal
Articles available online http://www.ijoer.in

Vol.2., Issue.4, 2014

RESEARCH ARTICLE

ISSN: 2321-7758

'SAFETY CHALLENGES IN OPPORTUNISTIC NETWORKS FOR DIFFERENT ATTACKS

ANJALI SHARMA[1], VISHAL WALIA[2], Dr. RAHUL MALHOTRA[3]

[1]Student Dept. of ECE RIEIT, Railmajra Punjab

[2]Associate professor Dept. of ECE RIEIT,Railmajra Punjab

[3]Director ,CTITR Jalander Punjab

Article Received: 12/08/2014 | Article Revised on: 22/08/2014 | Article Accepted on:28/08/2014

ANJALI SHARMA

ABSTRACT

An opportunistic network is one of the type of wireless network. Delay tolerant network is communication networking proposal which enables the communication in such an environment where end to end path may never be exist Mobile social networks (MSNs) are specific types of social media which consolidate the ability of Omni present connection for mobile users/devices to share user-centric data objects among interested users. Taking advantage of the characteristics of both social networks and opportunistic networks, MSNs are capable of providing an efficient and effective mobile environment for users to access, share, and distribute data. However, lack of a protective infrastructure in these networks has turned them into convenient targets for various perils. This is the main impulse why MSNs carry disparate and intricate safety concerns and embrace divergent safety challenging problems. In this paper, we aim to provide a clear categorization on safety challenges and a deep exploration over some recent solutions in MSNs. This work narrows the safety challenges and solution techniques down from opportunistic networks and delay tolerant networks (DTNs)

Keywords: Opportunistic, black hole ,Sybil attack ,virus attack and selective packet drop attack.

INTRODUCTION

Mobile Ad Hoc Networks (MANETs) feature self organizing and independent infrastructures, which make them an ideal choice for military uses such as communication and information sharing in battlefields. Although anonymity may not be a requirement in civil-oriented applications, it is critical in military applications (e.g., soldier communication).

Opportunistic Networks is a type of challenged networks. An opportunistic network is a sub-class of delay tolerant network where communication contacts are not constant, so an end-to-end path between the source and the destination may never exists. An opportunistic network may include cellular Base Stations offering Macro cell , Microcell, Pico cell, or coverage, as well as Wi-Fi access points , mostly connected through wireless networks. The devices included in an opportunistic network can be mobile phones, personal computers, cameras, etc. In opportunistic networks each node acts as a gateway which makes it much more

flexible than DTNs .Further more allowing nodes to connect and disconnect at will paves the way for a number of novel application scenarios in the field of mobile ad hoc networks. So far, the main focus of research on opportunistic networks has been on routing and forwarding issues, because finding routes towards the desired destination in such disconnected environments is regarded as the most compelling issue. Several concepts behind opportunistic networks come from the studies on Delay Tolerant Networks (DTNs) that have been conducted within the Internet Research Task Force and have led to the specification of the DTN architecture. The DTN architecture consists of a network of independent internets each characterized by Internet-like connectivity in within, but having only occasional communication opportunities among them, sometimes scheduled over time, some others completely random. Independent internets located apart from each other form so-called DTN regions and a system of DTN gateways is in charge of providing interconnection among them. Hence, in DTNs points of possible disconnections are known and isolated at gateways. Each internet relies on its own protocol stack that best suits the particular infrastructure, communication. They will exist temporarily, i.e. for the time frame necessary to support particular applications (requested in specific location and time). Applications can be related to the social networking and presume (derives from the combination of "producer" and "consumer") concepts as well as to the support of an enterprise (in a particular area and time interval) for developing and delivering products or digital services.

Opportunistic networking

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.

The Opportunistic network has the following features:-

- They are governed by operators through the provision of resources (e.g., spectrum available) and policies, as well as context/ profile information and knowledge, which is exploited for their creation/maintenance. At the lower layers, the operator designates the spectrum that will be used for the communication of the nodes of the opportunistic network (i.e. the spectrum derives through coordination with the infrastructure).In this respect, in principle, the bands will be licensed.
- The network layer capitalizes on context-, policy-, profile-, and knowledge-awareness to optimize routing and service/content delivery. In opportunistic networking no assumption is made on the existence of a complete path between two
- Nodes wishing to communicate. Source and destination nodes might never be connected to the same
- Network, at the same time. Nevertheless, opportunistic networking techniques allow such nodes to exchange messages between them. Usually, this comes at the price of additional delay in messages delivery, since messages are often buffered in the network waiting for a path towards the destination to be available. However, there is a wide range of applications able to tolerate this. Actually, this communication paradigm is reminiscent of widespread applications such as e-mailing.

LITERATURE SURVIVY

- **P. Krishna, N. H. Vaidya (1997)** presents in their paper that MANETs can divide in a number of clusters and each node in MANETs is a member of at least one cluster. There is a cluster head node in every cluster which monitors other node for a period of time. All nodes in a cluster reside with in same range with each other and cluster head have highest efficiency then other nodes. They also define the methods to select a cluster head .

- **D. Nain, N. Petigara, and H. Balakrishnan (2003)** studied about the *Mobile Relay Protocol.* MRP has been conceived to integrate pre-existing ad hoc routing protocols and manage message forwarding when no route towards the destination node of a message is found and the application that has generated the message can tolerate some form of extra delay. Messages that can be forwarded in opportunistic fashion are assigned two parameters: *x* and *y*. *x* represents the upper bound limit for the number of times the message can be relayed, i.e., the maximum number of relays that it can visit. Each time the message reaches a new relay node, *x* is decreased by one so as to correspond to the residual number of relays that it is allowed to visit from then on. On the other hand, represents the upper bound limit for the length of a multi-hop path towards the destination node according to a traditional routing protocol. Therefore, a message can overall traverse *x* hops over a non-connected path and *y* hops over a connected path (D. Nain, 2003)
- **S. Jain, K. Fall (2004)** found that routing as a big challenge in such a network which is work even in disconnected mode and message can only forward when node get an opportunity. It is a difficult to provide an efficient routing protocol, as routing performance is depends on the network topology. But in opportunistic network, topology information is absent. A node can only find the existence of another node when the come in their communication range. In such a scenario context base knowledge is best method to design a routing protocol for this type of network .
- **Chaintreau et al. (2006)** studied the transfer opportunities between mobile devices carried by humans by analyzing several user traces. They found that the distribution of the inter-contact time of a pair of devices, i.e., the time gap between two successive contacts, follows approximately a power law distribution. Also present a preliminary analysis of 2 user traces with a focus on statistical properties like node degree distribution and topological properties like cluster occurrences. (Chaintreau P. H., 2006)
- **PAPAJ Jan (2006)** find that the opportunistic network as a most challenging evolution of MANETs. Opportunistic network provide possibility to exchange message between nodes even in disconnected mode by forwarding the message packet to the neighbor node by the selection algorithm of opportunistic network, and message is move closer to the destination node, They introduce the basic security issues, described and there are displayed basic security mechanism and algorithms, they find that a strong and robust security solution is needed to transmission of data between source and destination node. In this article they present the security keys.
- **A.3 Zehua Wang** gives a noble approach in year 2012 for routing in opportunistic network. This paper proposed that The link quality variation of wireless channels has been a challenging issue in data communications until recent explicit exploration in utilizing this characteristic. The same broadcast transmission may be perceived significantly differently, and usually independently, by receivers at different geographic locations. Furthermore, even the same stationary receiver may experience drastic link quality fluctuation over time. The combination of link-quality variation with the broadcasting nature of wireless channels has revealed a direction in the research of wireless

networking, namely, cooperative communication. Research on cooperative communication started to attract interests in the community at the physical layer but more recently its importance and usability have also been realized at upper layers of the network protocol stack. In this article, we tackle the problem of opportunistic data transfer in mobile ad hoc networks. Our solution is called Cooperative Opportunistic Routing in Mobile Ad hoc Networks (CORMAN). Nodes in the network use a lightweight proactive source routing protocol to determine a list of intermediate nodes that the data packets should follow route to the destination. Here, when a data packet is broadcast by an upstream node and has happened to be received by a downstream node further along the route, it continues its way from there and thus will arrive at the destination node sooner.

DIFFERENT ATTACKS IN OPPORTUNISTIC NETWORK-BASED

There are also different types of attacks in opportunistic networks:-

A) **Viruses Attack**

B) **Selective packet drop**

C) **Black-hole**

D) Sybil attack

Viruses Attack:- A computer virus is a type of malware that propagates by inserting a copy of itself into and becoming part of another program. It spreads from one computer to another, leaving infections as it travels. Viruses can range in severity from causing mildly annoying effects to damaging data or software and causing denial-of-service conditions. Almost all viruses are attached to an executable file, which means the virus may exist on a system but will not be active or able to spread until a user runs or opens the malicious host file or program. When the host code is executed, the viral code is executed as well. Normally, the host program keeps functioning after it is infected by the virus. However, some viruses overwrite other programs with copies of themselves, which destroys the host program altogether. Viruses spread when the software or document they are attached to is transferred from one computer to another using the network, a disk, file sharing, or infected e-mail attachments.

Selective packet drop:-in a computer networking a packet drop attack or black hole attack is a type of denial-of-service attack in which a router that is supposed to relay packets instead discarded them. This usually occur from a router becoming compromised from a number of different causes. The packet drop attack can be frequency deployed to attack wireless ad hoc networking. Because wireless networking have a much different architecture than that of a typical wired network a host can broadcast that it has a short networking.

Black-hole Attack: Black-hole is a type of denial-of-service (DoS) attack which targets trust. In this type of attack, a malicious node, in reply to its given path request PREQ), sends a forged path replay packet to a source node that initiates the route discovery. This is because the malicious node pretends to be a destination node itself or an immediate neighbor of the destination node. As a result, the source node will forward all of its data packets to the malicious node describes an example of this attack. To prevent such an attack, Li and Das designed a trust-based framework and later integrated it with a large family of existing single-copy data forwarding.

Sybil attacks :-Another significant work to detect Sybil attacks was made in The main goal of this work is to assess a genuine user in MSNs with honest intentions by limiting the maximum number of Sybil independently. In addition, it encompasses two distinguished complementary appendages; explicit and implicit social trust.

Explicit social trust is based on consciously established friend ties and calculates trust as a function of hop distance and interconnection. It conveys trust which in terms of identity is not Sybil and verifies the honesty of the user authentication. Implicit social trust leverages mobility properties to convey trust in the originality of identities due to their persistency. Their further proposition was to optimize the trust level of the initial version of Pod Net. In this version, content publication was done anonymously, making it an ideal platform for spam and illegal contents to be spread. They proposed an integrated safe framework called Pod Net Sec which contains three types of channels, namely open, restricted, and closed channels as shown in closed channels allow private and encrypted dissemination of content in a limited group. Restricted channels only allow authorized users to publish content but everybody to consume it. Open channels allow every user to consume as well as create new content. Although this work mainly focuses on trust in Opp Nets, having the ability to maintain trust in an anonymous content-publication environment makes it possible to be implemented.

DEMONSTRATION OF SOME RECENT SAFETY SCHEMES IN TRUST CATEGORY IN MOBILE SOCIAL NETWORKS USED IN OPPORTUNISTIC NETWORK

Scheme	FUNCTIONALITY	**SYBIL ATTACK**	**black hole**	**Virus attack**	**Selective packet drop**
Social Trust	Confines the maximum number of Sybil independently using explicit and implicit trust	YES	NO	NO	NO
PodNetSec	Leverages trust layers in three channels by maintaining different level of restrictions for publishers.	YES	NO	NO	YES
SAMART	Allows credits to be distributed among nodes through a bundle forwarding cooperative manner without reliance on any tamper proof hardware.	YES	NO	NO	NO
SybilDefender	Detects Sybil nodes and the community around them by leveraging network topologies	YES	NO	YES	NO
SecuredTrus	Performs workload distribution by measuring trust with a load-balancing algorithm	NO	NO	NO	NO
Success	Enables all nodes to manage their own reputation and gives neighboring nodes the ability to monitor traffic by keeping track of each other's reputation	NO	NO	NO	NO
G2G	Forces faithful behavior to leave positive side-effect to improve performance by reducing message ratios.	NO	NO	NO	NO
Social-based Trust	Investigates the potential impact of lack of trust on node cooperation and leverages social information through six trust based filters.	NO	NO	NO	NO
MobiTrust	Establishes reliable and accurate trust using profile similarity, reputation, friendship	NO	NO	NO	YES
Data ForwarD	Blocks black-hole attacks by contributing positive forwarding message, a trust-based framework, and data forwarding protocol.	NO	YES	NO	NO/YES
RANOD	Monitors the forwarding behavior of a node using the number of times of previous encounters as the metric to select the next qualified forward	NO	YES	YES	YRS

REFERANCE

[1]. Anna Scaglione "Opportunistic Large Arrays: Cooperative Transmission in Wireless Multihop Ad Hoc Networks to Reach Far Distances" IEEE TRANSACTIONS ON SIGNAL PROCESSING, VOL. 51, NO. 8, AUGUST 2003.

[2]. Chiara Boldrini, Marco Conti, Andrea Passarella "Exploiting users' social relations to forward data in opportunistic Networks"1016/j.pmcj.2008.04.003 2008 Elsevier.

[3]. Zehua Wang "CORMAN: A Novel Cooperative Opportunistic Routing Scheme in Mobile Ad Hoc Networks" IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 30, NO. 2, FEBRUARY 2012.

[4]. J.P. Tower and T.D.C. Little "A Proposed Scheme for Epidemic Routing with Active Curing for Opportunistic Networks" In Proc.1st IEEE Intl. Workshop on Opportunistic Networking, Okinawa, Japan, March 2008.

[5]. Gokce Gorbil, Erol Gelenbe "Opportunistic Communications for Emergency Support Systems" 1877–0509 © 2011 Published byElsevier 10.1016/j.procs.2011.07.008.

[6]. B.Poonguzharselvi1 and V.Vetriselvi "Trust Framework for Data Forwarding in Opportunistic network Using Mobile Traces"International Journal of Wireless & Mobile Networks (IJWMN) Vol. 4, No. 6, December 2012.

[7]. Abdullatif Shikfa , Melek Önen , Refik Molva "Privacy and confidentiality in context-based and epidemic forwarding" 2010Published by Elsevier B.V:10.1016/j.comcom.2010.04.035

[8]. Abdullatif Shikfa and Melek Önen and Refik Molva "Local key management in opportunistic networks" Int. J. CommunicationNetworks and Distributed Systems, Vol. 9, Nos. 1/2, 2012.

[9]. Enrico Scalavino, Giovanni Russello and Rudi Ball "An Opportunistic Authority Evaluation Scheme for Data Security in CrisisManagement Scenarios" ASIACCS'10 April 13–16, 2010, Beijing, China.

[10]. Ram Ramanathan, Richard Hansen "Prioritized Epidemic Routing for Opportunistic Networks" June11, 2007, San Juan, PuertoRico, USA.

[11]. Pelusi, L., Passarella, A. and Conti, M. (2006) "Opportunistic networking: data forwarding in disconnected mobile ad hoc networks", IEEE Communications Magazine, Vol. 44, pp.134–141.

[12]. Thrasyvoulos Spyropoulos, Konstantinos Psounis, Cauligi S. Raghavendra "Efficient Routing in Intermittently Connected MobileNetworks: The Multiple-Copy Case" IEEE/ACM Transactions on Networking, Vol. 16, No. 1, February 2008.

[13]. Marmon Hussein Marmon, Saud Barak "Adaptive Priority Routing Protocol for DTN Networks" International Journal ofEngineering and Technology Volume 3 No. 3, March, 2013.

[14]. A. Vahdat and D. Becker, "Epidemic routing for partially-connected ad hoc networks" Duke University, Tech. Rep. CS-2000-06,Jul. 2000.

[15]. S. Jain, K. Fall, and R. Patra, "Routing in a delay tolerant network," in Proc. ACM SIGCOMM, Oct. 2004.

[16]. A. Doria M. Uden, and D. P. Pandey, Providing connectivity to the saami nomadic community, in Proceedings of the 2ndInternational Conference on Open Collaborative Design for Sustainable Innovation (dyd 02), Bangalore, India, Dec 2002.

[17]. A. Pentland , R. Fletcher, and A. A. Hasson, A road to universal broadband connectivity, in Proceedings of the 2nd International Conference on Open Collaborative Design for Sustainable Innovation (dyd 02), Bangalore, India, Dec 2002.

[18]. G. E. Prescott, S. A. Smith, and K. Moe, Real-time information system technology challenges for NASAs earth science enterprise,