International Journal of Research in Engineering, Science and Management
Volume-1, Issue-6, June 2018
www.ijresm.com

A Survey on Mobile Opportunistics Network: Challenges and Protocols

Rachana G Sunkad
M. Tech. Student, Department of Studies in Computer Science and Engineering, University BDT COE, Davangere, India

***Abstract*—Mobile Opportunistic Network is the modern kind of delay-tolerant networks (DTNs) in which mobile users interact which each other by sharing data. The mobile devices are considered as the nodes, these nodes communicate with each other when they are in certain communication range. There are various routing protocols used in oppnet for communication. Nodes store and carry the data to meet the required destination. One of the major challenges or we can say issue in mobile opportunistic network is trust, safety and privacy**

Index Terms—delay tolerant networks, encountering information, mobile opportunistic social networks

I. Introduction

The mobile computing has developed so much that there are various networks has been developed such as MANET, DTN, MOSN etc., Delay-Tolerant networking (DTN) is an approach to computer network architecture that seeks to address the technical issues in heterogeneous networks that may lack continuous network connectivity. Examples of such networks are those operating in mobile or extreme terrestrial environments, or planned networks in space. Opportunistic Mobile Social Networks (MSN) is a Kind of Delay-Tolerant Network (DTN) in which nodes are mobile with social characteristics.

In recent years, opportunistic mobile social networks emerged as a new mechanism of communications in wireless networks. The other communications of wireless networks are delay Tolerant networks (DTN) and MANET [4]. Unlike Mobile adhoc networks (MANETs) that require end-to-end communication paths for message exchange, the communication in opportunistic mobile social networks takes place on the establishment of opportunistic contacts among mobile nodes, without availability of end-to-end message routing paths. As the mobile devices make only contact when humans come into contact, such networks are tightly coupled with human social networks [4]. Therefore opportunistic mobile social networks exploit the human behaviors and social relationships to build more efficient and trustworthy message dissemination scheme. Involving humans in the cloud computing and wireless connection loops becomes an alternation for information retrieval deriving from observing humans behaviors and inter-activities over various social networks and mobile apps. The mobile devices are represented as nodes, as human mobility each nodes moves, when there in a range of communication nodes communicate with each other. This activity does not provide the privacy which is the most important criteria in the network. Thus trust, safety and privacy becomes a major challenges of mobile opportunitics networks if the problems aren't solved nodes are more prone for attacks. The routing in Mobile Opportunistics Network has various ways. The communication between two mobile nodes is primarily vary with the protocols used for routing the packets. A wireless routing protocol is used in oppnet i.e., forwarding based routing protocol and flooding based routing protocol which is described in section iv.

II. Challenges in Opportunistics Networks

- Secure routing: A list of trusted devices need to be maintained. They can be owned institutes such as police stations, government offices, hospitals, universities, etc. The route must be chosen that passes through maximum trusted devices. But this is very challenging. For this purpose secret keys and digital signatures can be used.
- Node privacy: Privacy of node can be guaranteed by authentication and authorization, intrusion prevention and intrusion detection. Privacy of opportunistic network need to be maintained as malicious nodes can join the network.
- Data Privacy: Encryption is a way of providing data privacy. Public key cryptography can be used this case. Here the controller can encrypt data with public key and devices can decrypt it with their private keys. A secure mechanism is needed for the broadcast of the public key, otherwise a malicious device can also distribute its own public key.
- Identify attacks: The attacks can be Man in the middle attack, packet dropping, DOS (Denial of Service), ID spoofing, Intrusion Detection.

III. Related Works

A. Prefilter: An efficient privacy-preserving relay filtering scheme for delay tolerant networks

Without direct path, information delivery in sparse delay tolerant networks (DTNs) typically relies on intermittent relays, making the transmission not only unreliable but also time consuming. To make the matter even worse, the source nodes may transmit some encrypted "junk" information, similar as the spam emails in current mail systems, to the destinations; without effective control, the delivery of encrypted junk information would significantly consume the

precious resource of DTN and accordingly throttle the network efficiency. To address this challenging issue, propose PReFilter, an efficient privacy-preserving relay filter scheme to prevent the relay of encrypted junk information early in DTNs. In PReFilter, each node maintains a specific filtering policy based on its interests, and distributes this policy to a group of "friends" in the network in advance. By applying the filtering policy, the friends can filter the junk packets which are heading to the node during the relay. Note that the keywords in the filtering policy may disclose the node's interest/preference to some extent, harming the privacy of nodes, a privacy-preserving filtering policy distribution technique is introduced, which will keep the sensitive keywords secret in the filtering policy. Through detailed security analysis, we demonstrate that PReFilter can prevent strong privacy-curious adversaries from learning the filtering keywords, and discourage a weak privacy-curious friend to guess the filtering keywords from the filtering policy. In addition, with extensive simulations, we show that PReFilter is not only effective in the filtering of junk packets but also significantly improve the network performance with the dramatically reduced delivery cost due to the junk packets.

B. Utilizing social links for location privacy in opportunistic delay-tolerant networks

This paper is concerned with improving location-privacy for users accessing location-based services in opportunistic DTNs. We design a protocol that offers location privacy through request/reply location obfuscation technique that uses the nodes' own social network to drive the forwarding heuristic. We propose a fully distributed social-based location privacy protocol (SLPD) that utilizes social ties between nodes to ensure K-Anonymity, i.e. the requesting node's locations cannot be determined from at least k-1 other nodes in its social network. We evaluate SLPD using extensive simulations and real connectivity data traces. We compare our results to a benchmark protocol that requires centralized trusted server. We show that our distributed protocol is applicable to DTNs with various mobility patterns, and provides the user with the required privacy at less than 30% of the privacy range we define. SLPD achieves success ratios similar to the ones obtained using centralized benchmark solutions up to 15% privacy requirements.

IV. Mobile Opportunistics Social Networks

In Opportunistic Networks, nodes can only forward the message when they get in opportunity to send it. Opportunity means that a node is able to forward the message only when the intermediate nodes come in its range of communication [3]. The node which wants to send the message needs a neighbour node which is closest to it and lies in its range. Now the message is carried by the neighbour node and the same process is now used by the neighbour node to forward the message. This process goes on till the data reaches the intended destination node. The following figures show how communication takes place. The figures involve the use of different network clusters to depict communication.

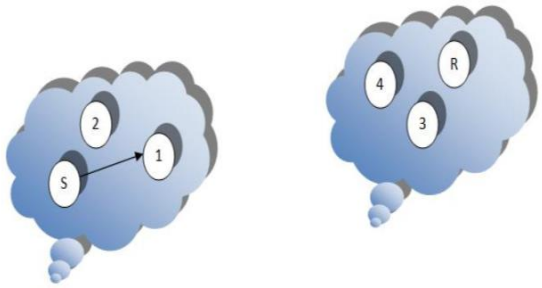

Fig. 1. Message forwarding to an intermediate node by source

In Fig. 1, Node S (source node), wants to send the message to the node R (destination node), node S forwards the message to only that node which is in its range. Node 1 and Node 2 are in the communication range of source node, so the source node passes the message to a node in its communication range. Node S forwards the message to Node 1.

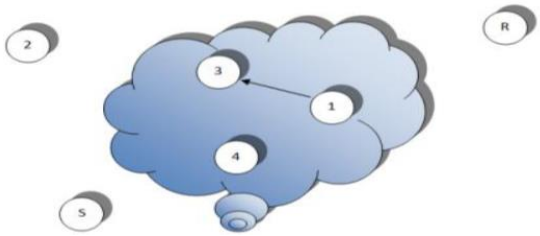

Fig. 2. Message forwarding between intermediate nodes

In Fig. 2, Node 1 leaves the range of source node, and stores the message with it until another node comes in its range. Here, Node 4 and Node 3 appear in the range of communication of Node 1. And Node 1 passes the message to the Node 3.

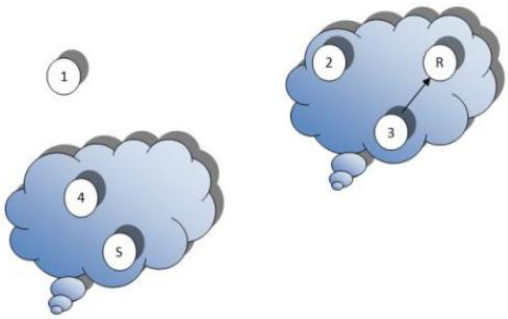

Fig. 3. Message forwarding between intermediate node and destination

In Fig 3, Node 3 is now in the range of communication of Node R (may be Node 3 moves or Node R is moves to be in range) and forward the message to destination Node R. If Node R does not appear within the range of Node 3 then Node 3 stores the message and when it gets opportunity, forwards it to another node. Here the Store and Forward approach is used where the data is store in the node, node carry the data and forwards to the intended destination. There can be one or many intermediate nodes in the midway of the source and the destination. The links between nodes are temporary. Activation and deactivation of nodes changes can change the topology of the network. During the communication there can the chance

of disclosing the nodes real id since the nodes communicate with each other using their real id. This causes the privacy of the node is at the danger, it is more prone for attacks by intruders or malicious node.

Routing Protocols:

Traditional MANET routing cannot be used for such networks. OPPNET routing protocols (as in Figure 4) can be classified as [3].

1. Forwarding-based approach: This approach is based on the type of knowledge node uses to select the best path for transmission to the destination node. It can further be classifies into:
   a. Direct transmission: Here, the source node generates a message and it holds it until the message reaches its destination. It consists of less overheads and long delays.
   b. Location-based - Here, to pass the message, nodes choose those nodes which are closest to the destination. MobySpace is an example of this. It uses nodes mobility patters for routing. The measure of closeness represents the probability that the nodes will come into contact with each other.
   c. Knowledge-based: Here selection of the nodes depends on the knowledge of the source, network or the intermediate nodes. Context Aware Routing (CAR) is an example of this. It is a general framework for the evaluation and prediction of context information, aimed at achieving efficient and timely delivery of messages.

2. Flooding-based approach - Here, every node broadcasts the message to all its neighbouring nodes.
   a. Epidemic routing: Epidemic routing scheme is the solution to send a message when the context information is not present. It uses pair-wise exchange of messages between the nodes. The disadvantage is that congestion occurs due to flooding.
   b. Estimate/prediction routing: Here, nodes estimate the probability of each link to destination and then use the information to select the nodes for forwarding purposes. PROPHET is an example of this type of routing which means Probabilistic Routing Protocol using History of Encounter and Transitivity. If a user visits a node many times, there is a possibility that it will visit that node again. Delivery predictability metric is maintained at every node.

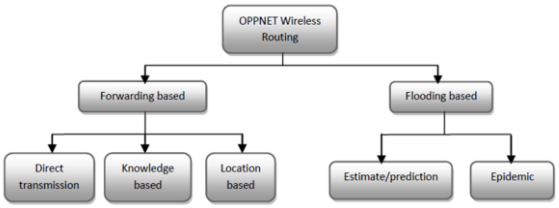

Fig. 4. Classification of OPPNET routing protocols

V. Conclusion

Opportunistics network takes the idea of Delay-Tolerant Network which main aim is to provide the efficient transmission of the data. It uses the store and Forward approach i.e., nodes store the data carry and forward it to the Destination. This communication in wireless network does not require the end –to-end communication. When the nodes meet in communication range they communicate with their nodes id which causes privacy concern. Privacy is the major challenge in the opportunistic network. The various approaches are carried out in research to maintain the privacy in the Oppnet. Node communicate with each other through neighbor nodes using certain routing protocols.

References

[1] P. Hui, E. Yoneki, S. Y. Chan, and J. Crowcroft, "Distributed community detection in delay tolerant networks," in Proc. MobiArch, 2007, Art. no. 7.

[2] R. Lu *et al.*, "Prefilter: An efficient privacy-preserving relay filtering scheme for delay tolerant networks," in *Proc. IEEE INFOCOM*, Mar. 2012, pp. 1395–1403.

[3] S. Zakhary and M. Radenkovic, "Utilizing social links for location privacy in opportunistic delay-tolerant networks," in *Proc. IEEE ICC*, Jan. 2012, pp. 1059–1063.

[4] Navneet Kaur,Gauri Mathur, "Opportunistic Networks: A Review," in *IOSR Journal of Computer Engineering(IOSR-JCE)*,Volume 18,Issue 2, Mar./Apr. 2016, pp. 20–26.