www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 3 Issue 5 may, 2014 Page No. 6104-6108

FSR: Ferry-based Secure Routing Algorithm for Delay Tolerant Networks

Sapna Grover, Aditya Pancholi, Sonika Arora
sapna.grover5@gmail.com ,aditya.cs.du@gmail.com, sonika.ta@gmail.com
Assistant Professor, University of Delhi, India

Abstract: *A delay tolerant network(DTN) is a collection of infrastructure-less nodes, with no communication medium. These nodes cooperate dynamically to meets certain immediate needs. Therefore, each node acts as a router also beside being merely a host. Security issues have thus become more challenging in these networks due to its dynamic nature. Thus these networks are vulnerable to different kinds of attacks because of which security has always been a major concern.*

This paper uses ferry-based [11] mechanism for providing security and maintaining consistency throughout the network.

1. Introduction

Mobile Ad-Hoc networks (MANETs) [1] is a class of networks that lacks fixed infrastructure like a base station and a communication medium. The nodes are completely mobile and hence routing is hop-to-hop. A path between sender and receiver is assumed if it does not exists. However, if there is no assurance that a path will ever exist in future, then the network is called a Delay Tolerant Network(DTN) [2].

In DTNs, determination of next hop node is opportunistic in nature. A message is transmitted hop-by-hop upon encountering the next best node. An intermediate node stores the message in its buffer until a connection with the next hop is established. These above mentioned properties make routing protocols in DTNs follow “store and forward” strategy.

Routing in Ad-hoc networks has been extensively studied in past. Common routing protocols for MANETS such as AODV (Ad hoc on-demand distance vector routing) [3] and DSR (Dynamic Source Routing) [4] cannot establish route in case of DTNs because of the lack of presence of an end-to-end path. Therefore, routing protocols in DTNs first try to find the next best node amongst the one to whom it is connected and then forward the message.

Lindgren et. al [6] gave PRoPHET protocol which forwards messages to nodes on the basis of its probability of delivering the message. This delivery probability is measured in terms of history of nodes' encounters and transitive relation among their connections. Transitivity makes exchange of messages possible between two nodes which are not connected directly with each other.

Another routing technique, CAR (Context-aware Adaptive Routing) by Musolesi et. al [7] intelligently forwards messages to intermediate carrier nodes, which are chosen on the basis of a

function defined on its context attributes. Kalman Filter Prediction [8] technique is then applied on the calculated function value to improvise the selection of carrier node.

Dini et. al [9] extend the work of Musolesi et. al and introduce the concept of reputation of a node, which is a local notion of a node. This reputation is then used to select the carrier nodes. The protocol presented provides security against malicious nodes also. Chuah et. al [11] also gave a ferry-based protocol to detect malicious nodes. Certain nodes act as trusted examiner nodes (called ferries) which travel along fixed routes in the network and provide security to all the other nodes on the basis of delivery probability and encounter information provided by them to ferries.

Another technique to increase the chances of successful delivery of the message to the destination is to replicate the message and send it via all possible available routes. This technique is called Epidemic routing and is given by Vahdat et. al [11].

MaxProp routing protocol given by Burgess et. al [5] maximizes the chances of delivery of a message by choosing a route to the destination with the smallest cost. The protocol described is a multi-copy routing protocol and prioritizes the packets residing in the buffer of a node to decide the order of forwarding.

On the similar lines of MaxProp protocol, we give a Ferry-based Routing Algorithm which efficiently chooses the best path to the destination and provides additional security against malicious nodes.

The rest of the paper is organized as follows: Section 2 briefly summarizes the MaxProp protocol. Section 3 describes our algorithm in detail. Conclusion and future work is described in section 4.

2. MAXPROP Protocol

MaxProp protocol is a competent routing protocol to transmit messages in a DTN. The protocol is based on creating multiple copies of a packet and is well suited for the situations where transfer duration or storage space is limited. The protocol assumes that a node has infinite buffer space for the messages originated by itself but limited space for the messages received from other nodes. Since transfer opportunities are limited in terms of duration and bandwidth, in order to avoid their misuse or overuse, the protocol sends acknowledgments all over the network, not just to the source.

MaxProp stores and forwards the packets in a particular order, decided on the basis of the cost assigned to their destination. This cost is an estimate of delivery likelihood of all nodes in the path and is calculated by integrating the cost of reaching all the intermediate nodes including the final destination. The cost for a path is the sum of probabilities that each link on the path specified does not occur, which is nothing but the probability that each such connection does occur, subtracted from one.

MaxProp transmits packets in a pre-defined specific priority order. A higher priority is given to new packets, whereas packets with hop counts lower than a given threshold are deleted accordingly. Packets with the highest priority are transmitted first whereas packets with the lowest priority are the first to be deleted. When two packets arrive with the same cost to the destination, tie is broken by giving higher priority to the packet that has traveled fewer hops.

According to the priority order, a message destined for a neighboring node is delivered first. Second, the routing table is exchanged between

peers. Third priority is given to the acknowledgement messages. In the fourth chance, the packets that have not traversed far in the network, i.e., whose hop count is more than the threshold are given priority. At last, all the remaining un-transmitted packets are considered for transmission.

In MaxProp, nodes keep copies of messages even after forwarding them (in lieu of a better path or meeting the destination node itself). So there is an urge to manage buffer of a node so as to make space for new incoming packets and deleting the older ones. A node deletes a copy of the packet in either of the three mutually exclusive cases: if a copy of it is delivered to the destination and acknowledgement is received, or if there does not exists any route with enough bandwidth between the node and the destination of the packet, or the node is almost sure that a copy of the packet will be delivered to the destination in future even if it drops it.

3. FSR: Ferry-based Secure Routing Algorithm

In this section, we describe a protocol which is an improved algorithm on the similar lines as MaxProp algorithm. Our algorithm is highly optimized in comparison to standard MaxProp protocol and it is also robust against attacks from malicious nodes. We assume that each node has infinite buffer capacity, acknowledgements are forwarded using epidemic routing. Apart from these nodes, there are certain special nodes which do not participate in data transfer but helps in maintaining consistency and authenticity of the network.

3.1 Preliminaries

For the sake of brevity, we describe certain terms and concepts that will be used extensively by our algorithm.

Let Π be the set of all nodes in the network. We use several mechanisms in concert to increase the delivery rate, lower latency of delivered packets and to detect malicious nodes.

Definition1 (Delivery Certainty). For every node $v \in \Pi$, we define delivery certainty $f(v,u)$ for every other node u. Delivery Certainty $f(v,u) \in [0,1]$ defines the probability that u will be the next node to come in contact with v.

For all nodes $f(v,u)$ is initially set to $1/(|\Pi|-1)$. When a node u is encountered, $f(v,u)$ is incremented by some positive value $0 \leq \delta \leq 1$ and then all values of $f(v,u)$ are re-normalized. This technique is often called incremental averaging [5]. This helps to lower the $f(v,u)$ values for nodes that are seen infrequently over time.

This can be explained with the help of a small example. Let for a DTN with four nodes (n_1, n_2, n_3 and n_4), initially node n_1 has $f(n_1,n_2)= f(n_1,n_3)= f(n_1,n_4)=1/3$ and $\delta=1/3$. Upon encountering node n_3, the value of $f(n_1,n_3)$ is incremented to 2/3 and after re-normalization the values become $f(n_1,n_2)=1/4$, $f(n_1,n_3)=1/2$, $f(n_1,n_4)=1/4$ respectively.

3.2 Ferry based centralized authority

Consider the case where a node or a set of nodes could be compromised, thus a set of certified nodes called ferry nodes are used to authenticate every node in the network. The entire geographical area is divided into multiple cells and every ferry nodes patrols some cells via a fixed path. Together, these ferry nodes cover the entire geographical area.

The ferry node passes through the center of each cell, it stops there and broadcasts a secret message that each legitimate node knows how to decipher. This can be done by having the ferry encrypt the message using a private key and

assuming that all legitimate nodes know the public key of the ferry. Upon receiving the secret message, each legitimate node shares its encounter and delivery predictability information it has with the ferry. The ferry correlates such information from all nodes to identify any potential malicious nodes.

As a single ferry node may not be able to cover the entire geographical area, thus there can be multiple ferry nodes who need to share gathered information with each other. Thus, there are some storage nodes across the network that help in facilitating the same. Also, there are special nodes called probe nodes which move between storage nodes. These probe nodes maintain consistency among the information gathered from storage nodes.

3.3 Malicious Meter

The centralized authentication mechanism tries to identify malicious characteristics of every node in the network. It keeps a malicious parameter $m(v) \in [0,1]$ for each node v in the network and a centralized malicious meter φ. Higher value of m(v) indicates higher probability that the node is malicious. If the value of m(v) goes beyond φ, the node is marked as malicious.

3.4 Routing Graph

The storage nodes maintain a routing graph for the entire DTN. For every node *v*, there is a vertex in the graph. And between every pair of vertices u,v ; there are edges (u,v) and (v,u) in the routing graph. The weight of the edge (u,v) is set to (1-*f(u,v))*m(v)*. Higher value of *f(u,v)* and lower value of *m(v)* indicates that *v* is a very good forwarding node, hence we associate a lower weight to the corresponding edge.

Whenever a source node *s* wants to send a packet to the destination *d*, it requests the ferry node to guide a path to the destination. Based on updated routing graph, ferry collects the delivery probability and encounter information from the storage node.

Ferry calculates shortest path from *s* to *d* in its routing graph, and provides this entire path. This path is appended in the packet header and is used for the transmission. Whenever some intermediate node receives a packet, it looks for the next hop from the header and forwards the packet only to that node.

Whenever a device is declared malicious or goes out of the network, it is removed from the routing graph and is never considered for transmission.

3.5 Parking Lot Problem

Key problem with the traditional MaxProp algorithm is that delivery certainty is maintained and updated by the nodes themselves. If a node faces re-connections due to flaky Wi-Fi conditions, it will be counted as a new encounter every time. This is very similar to the theoretically postulated parking lot problem. This will shoot up the delivery certainty between these pair of nodes, which can be exploited by a malicious node to attract packets towards itself.

The above mentioned problem is handled by the following modification. Instead of each node maintaining its own delivery certainty, we make the storage nodes store this information. Whenever two nodes come in contact they inform the ferry node about the same. Upon getting this information, ferry node validates it and updates the routing graph. Reincarnation of the same connections can be easily considered as one by the ferry node thus resolving the parking lot problem.

4. Conclusion

In this paper, we presented a ferry-based secure algorithm for routing in DTNs. The algorithm effectively finds the shortest available path to the destination with the help of a centralized mechanism. Our algorithm also provides security against malicious node in the network with the help of certain certified ferry nodes. With the assistance of these nodes, malicious nodes are easily identified and black-listed from transmission process.

References

[1] Abdul Shabbir, Anasuri Sunil Kumar (January 2012). "An Efficient Authentication Protocol for Security in MANETs". *IJCCT* 3 (1): 71–74.

[2] Artemios G. Voyiatzis, A Survey of Delay- and Disruption-Tolerant Networking Applications, Journal of Internet Engineering, Vol. 5, No. 1, June 2012, 331-344.

[3] C. E. Perkins and E. M. Royer. Ad hoc on-demand distance vector routing. In The Second IEEE Workshop on Mobile Computing Systems and Applications, February 1999.

[4] D. B. Johnson and D. A. Maltz. Mobile Computing, chapter Dynamic source routing in ad hoc wireless networks, pages 153–181. Kluwer Academic Publishers, February 1996.

[5] John Burgess, Brian Gallagher, David Jensen, and Brian Neil Levine. MaxProp: Routing for vehicle-based disruption-tolerant networks. In Proc. IEEE INFOCOM, April 2006.

[6] A. Lindgren, A. Doria, and O. Scheln. Probabilistic Routing in Intermittently Connected Networks. In Proc. Workshop on Service Assurance with Partial and Intermittent Resources, August 2004.

[7] M. Musolesi, C. Mascolo, Car: context-aware adaptive routing for delay-tolerant mobile networks, IEEE Transactions on Mobile Computing 8 (2009) 246–260.

[8] R. E. Kalman, “A new approach to linear filtering and prediction problems,” Transactions of the ASME Journal of Basic Engineering, March 1960.

[9] G. Dini, A.L. Duca, Towards a reputation-based routing protocol to contrast blackholes in a delay tolerant network, http://www.journals.elsevier.com /ad-hoc-networks, March 2012.

[10] A. Vahdat, D. Becker, Epidemic Routing for Partially Connected AdHoc Networks, Technical Report, Department of Computer Science, Duke University, 2000.

[11] M. Chuah, P. Yang, and J. Han, “A ferry-based intrusion detection scheme for sparsely connected adhoc networks,” in Proceedings of first workshop on security for emerging ubiquotous computing, 2007.