Journal of Mobile Communication
MEDWELL PUBLICATIONS

Detecting Mean Performance using Connectivity Information with NCPR in MANET

S. Madhurikkha
Jeppiaar Engineering College, Chennai 119, India

Key words: MANET, security design architecture, connectivity information, NCPR, predominantly

Corresponding Author:
S. Madhurikkha
Jeppiaar Engineering College, Chennai 119, India

Page No.: 28-33
Volume: 14, Issue 4, 2020
ISSN: 1990-794x
Journal of Moblie Communication

Abstract: Mobile Ad-hoc networks are predominantly deployed in emergency and military networks. Though, MANETs are very useful and have advantages over other wired and wireless networks, they are susceptible to a wide range of attacks and require stringent security and privacy measures. Research has so far focused on developing secure fail safe protocols for MANETs but so, far very little attention has been given to data plane and information that we can extract about the actual communication links. Routing information may be validated using data path information to provide high security levels to wireless networks. In this study, we use simulation methods to track and validate mobile node connectivity in order to identify potential malicious behaviour.

INTRODUCTION

Mobile Ad-hoc networks are increasingly prevalent and are widely used, especially for military operations and civil rapid-deployment networks for emergency rescue, disaster relief and law enforcement. Their advantages include versatile use and are particularly known for their flexibility and mobility. They are an efficient pattern for multicast communication as well. MANETs are however, vulnerable to attacks ranging from eavesdropping to active interfering.

MANETs have unique characteristics and we need to employ different techniques than other wired networks to deal with the security issues. Each mobile ad-hoc node can act as both a packet and router. During message transfer each node discovers and transfers information to the next hop until their final destination is reached. Unfortunately not all nodes can be trusted in hostile MANET environments mobile nodes face the risk of getting in the wrong hands and being misused. Even a few malicious nodes can deem the entire network inoperable by exhausting all network and power resources.

Therefore, designing a MANET network with security features is healthier rather than solving specific problems by adding more and more defence features. We consider all nodes to be potentially malicious by default.

All connectivity information of all nodes is gathered and recorded, so that, information can be used to distinguish fake connectivity or detect whether an unusually large number of information is being transferred one node. The information changes in the network cannot be constantly determined to the ever changing topology of the network. There are two sources that provide connectivity information in the network, i.e., the control plane and the data plane.

Routing messages exchange between nodes for connectivity information through data plane. Data transmission occurs along paths in the MANET that only have valid links implicitly represent actual connectivity information through control plane. The information obtained is validated against each source and verified. Verification and validation is the first step in eliminating discrepancies and identifying and isolation malicious nodes.

In this study we concentrate on connectivity information and how we can extract the information in an efficient way through observing a data plane. The objective is to:

- Use a space efficient structure to extract the connectivity information of each individual node. This has to be done quickly
- Store information by carrying the least possible amount of data inside the packets using header space

LITERATURE REVIEW

MANETS are susceptible to several types of attacks due to their mobile and dynamic nature. Existing communication paths can be disrupted or a peer can be swamped with fake communication requests by external attackers or malicious insiders[1]. Due to these vulnerabilities mobile ad hoc network security is an active area of research. Plenty of solutions have been proposed to design security protocols for routing[2-4].

MANETS require high security requirements and an ongoing effort has come up with a built in network security architecture. Resource usage is controlled by using a capability based mechanism which assigns a capability for each node to enforce[5,6]. Network design architectures with intrinsic assurances have also been proposed[7]. In this, nodes require explicit authorization before they can connect with other nodes. So, it is important to identify which connectivity information can be trusted. We have also proposed many methods for extracting topology information and discovering the paths that are actually taken in the network[8, 9].

Network tomography is an efficient and popular method used to extract information about the nodes or peers existing inside a network[10]. It is used to reveal network internal characteristics based on end-to-end measurements. To infer the multicast tree, topology reconstruction techniques based on end-to-end delays of multicast traffic are proposed. Probe packets are sent from some source towards multiple destinations, each pair of nodes keeps track of the packets received. Information about packet loss or delay of multiple links is shared by the nodes on which multiple links converge. A new network tree is constructed by the correlation of the received information and it's comparison through statistical methods.

A solution to the topology discovery problem can be the use of mobile agents. A mobile agent is a controllable network that can that can traverse over a network and performs operations such as node visits while cooperating with other mobile agents as well. Mobile agent deployment has found to be very extremely useful in large networks for its efficiency and scalability. Keeping this in mind many mobile agents are generated in the network to collect topology information. It is gathered as they travel from node to node periodically and transfer it back to a centralized management station[11].

Chandra and his associates[12] proposed a topology discovery method for hybrid networks. These networks, having wired and wireless links, are constructed from the perspective of each individual node. It requires each node to have a description of the entire topology. Their algorithm uses a spanning tree with a bottom-down approach. By the end of its execution the root has received the response message from all its children and is capable in reconstructing the topology of the network. It turns out that this proposition by Chandra and his associates is very accurate and discovers 100% of all nodes and links in the network.

Whereas the way to get hold of topology information from the control plane has been well studied in the perspective of routing protocols, the data plane, where the actual information exchange takes place, has received very little thought. Our work focuses on recording node connectivity information in the forwarding plane of the network. Prior work in this field has compared a number of data structures to keep records of taken paths[13]. However, the size of data records stored inside every 0packet makes it unrealistic to use. Furthermore, that scheme provides only limited topology information. To be able to record all possible paths, traffic would need to negotiate all possible links and end up at a single node, which is an unlikely scenario.

We propose a scheme where the need to store large path records in the packets themselves is not required. The connectivity information is kept inside each individual peer, combining these lists provides a complete view of the network topology. This approach requires changes in packet forwarding and header routine. This is a reasonable assumption since the security design requires many other additional changes if a secure MANET is to be created.

OVERVIEW OF AODV AND NCRPROUTING PROTOCOLS

The existing system uses Ad Hoc On-Demand Distance Vector Routing (AODV) and the proposed system uses Neighbour Coverage Based Probabilistic Rebroadcast Protocol (NCPR).

AODV routing protocol: Ad Hoc On-Demand Distance Vector Routing protocol is an on-demand route possession system where nodes do not keep any routing information and also not undertake any periodic routing table exchanges. It is one of the most important reactive routing protocols. The AODV establishes routes between

nodes only when a node needs to send out data. Otherwise the network is idle. The primary objectives of AODV are: To execute path discovery process when it is of need. AODV uses broadcast route discovery mechanism. To distinguish between dynamic connectivity of neighbourhood nodes and general topology maintenance. To inform neighbouring mobile about changes in local connectivity to those that are likely to need the information. While AODV is fast, it is easily vulnerable to attacks as the public key is exchanged between nodes without any precaution or background check.

NCPR routing protocol: Neighbour coverage based probabilistic rebroadcast is a combination of neighbour coverage which is a type of coverage where a node keeps interacts with its neighbour nodes prior to sending data to know its neighbour's public as well as private keys and update it in the routing table and probabilistic methods which use random probability to assign node information such as public and private keys to cluster heads. Two key factors are necessary to effectively make use of neighbour coverage knowledge and to find out rebroadcast order. They are rebroadcast delay which is a delay method used before getting more accurate additional coverage ratio, which in turn can be achieved by rebroadcast probability. Connectivity factor is used to determine the number of neighbours who should Receive the Route Request (RREQ), for stabilizing connectivity and for minimizing the retransmission of the same RREQs. By combining the additional coverage ratio and the connectivity factor, rebroadcast probability is established which helps in reducing the number of rebroadcasts and to improve the routing function.

METHODOLOGY USED AND IMPLEMENTATION

Working: The existing system uses AODV but to overcome the security deficiencies we propose a method using NCPR. This protocol is applicable to every individual node which collects the connectivity information from each neighbouring node. Each cluster of nodes appoints a cluster head. This cluster head forwards the data to another regions cluster head. The appointing node refers the routing table for the private and public key. If the keys differ from the original, then nodes which are altered are considered to be malicious nodes.

These malicious nodes are generally found to be in a cluster. This cluster is isolated from the other nodes, so as to ensure data transmission does not take place with the malicious nodes. The source node considers the routing table for the second best path which doesn't include the infected nodes. The data is then sent along that path.

After data transmission the network attempts to revive the malicious nodes trying to restore normality. If the attempt to revive the network is successful then new private and public keys are assigned and the routing table is updated. However, if it fails the nodes are isolated from the network NCPR is a two stage process (Fig. 1). They are:

Rebroadcast delay: The order in which forwarding takes place is found using Rebroadcast Delay. If a node has more common neighbours with its pervious node, then the delay will be low. Other neighbours will know this information if the node continues to retransmit the packet.

Node pi has more neighbours uncovered by the RREQ packet from s because when node pi rebroadcasts the RREQ packet, it reaches more neighbour nodes. To Compute the Uncovered Neighbours (UCN) set U(pi) of node pi as follows:

$$U(pi) = N(pi) - [N(pi) \cap N(s)] - \{s\} \quad (1)$$

The N(s) and N(pi) are the neighbours sets of nodes. s sends a RREQ packet to node pi. According to Eq. 1. Rebroadcast delay must be found out by each node so that

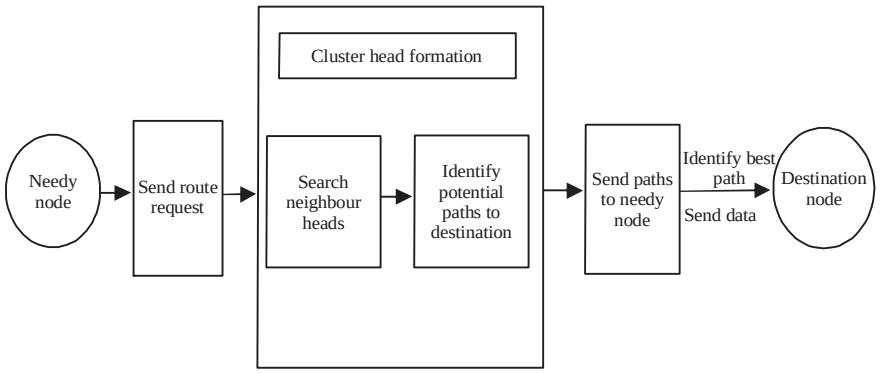

Fig. 1: Architecture diagram of the proposed system

channel collision can be avoided. When one node finds the rebroadcast delay, all its neighbours will calculate the delay as well. The node calculates by checking neighbour list of RREQ packet and its own neighbour list. The rebroadcast delay Td(pi) of node pi is defined as follows:

$$Tp(ni) = 1 - \frac{|N(S) \cap N(ni)|}{|N(S)|} \quad (2)$$

where, Max Delay is a small constant delay, Tp (pi) is the delay ratio of node pi and |•| is the number of elements in a set.

Rebroadcast probability: The rebroadcast probability is the combination of two factors: Additional coverage ratio: It is the ratio of nodes that should be covered by a single broadcast to the total number of neighbours and Connectivity factor: It is the relationship of network connectivity and the number of neighbours of a given node that are additionally covered by the node which has a more rebroadcast. Node ni could further adjust its UCN set according to the neighbour list in the RREQ packet from nj. Then the U(ni) can be adjusted as follows:

$$U(ni) = U(ni) - [U(ni) \cap N(nj)] \quad (3)$$

The additional coverage ratio Cr(ni):

$$Cr(ni) = |U(ni)| |N(ni)| \quad (4)$$

Connectivity factor can be defined as:

$$Cf(ni) = Nc |N(ni)| \quad (5)$$

Nc = 5.1774 log n, the n is the number of nodes in the network. Combining the additional coverage ratio and connectivity factor, to obtain the rebroadcast probability Pre (ni) of node ni:

$$Pre(ni) = Cf(ni) \cdot Cr(ni) \quad (6)$$

where, if the Pre (ni) is>1 , to set the Pre (ni) to 1.

Simulations: The network is simulated using AO DV and NCPR and evaluated based on the following criteria:

Package delivery ratio: The number of packets sent from the source node to the numb er of packets received at the destination node (Fig. 2 and 3). The simulation results show that the ratio is greater in NCPR when compared to AODV.

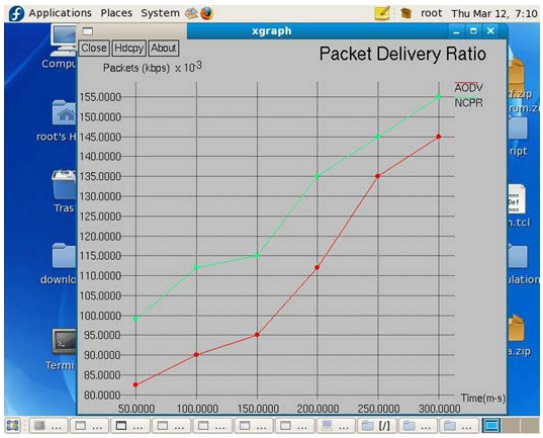

Fig. 2: Packet delivery ratio graph

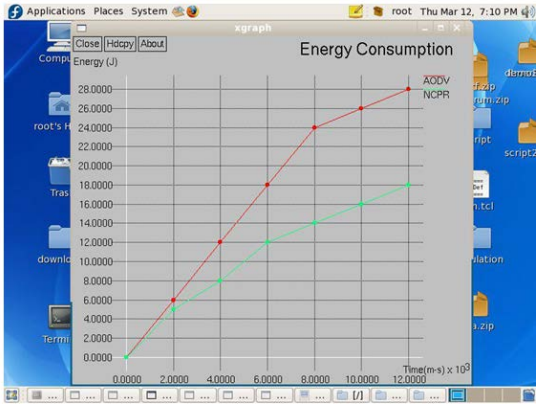

Fig. 3: Energy Consumption graph

Energy consumption: The energy consumed during transmissi on of data from one node to another is known as energy consumption. As the nodes use NCPR, each node knows the transmission details of its neighbour node. This leads to lesser power consumption than the traditional AODV.

End-to-end delay: The time taken for the data packet to move from one node to another between th e source node and the destination node and the delays involved is known as end-to-end delay (Fig. 4). For an efficient syste m, the end-to-end delay should be low. From the simulations, we can clearly see that the delay is less in NCPR than in AODV.

Throughput: The number of packets successfully delivered in a given time is known as throughput. For an efficient syste m throughput should be high. From the simulation you can see that NCPR has higher throughput than AODV (Fig. 5).

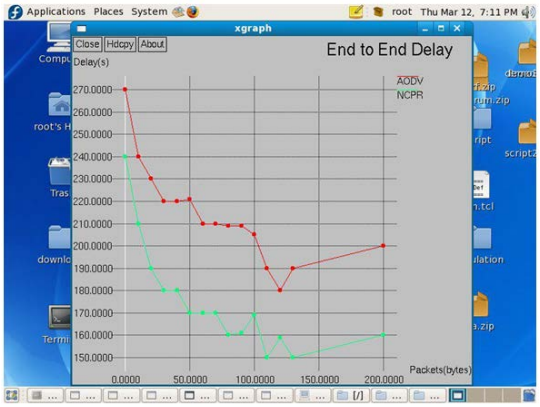

Fig. 4: End-to-end delay graph

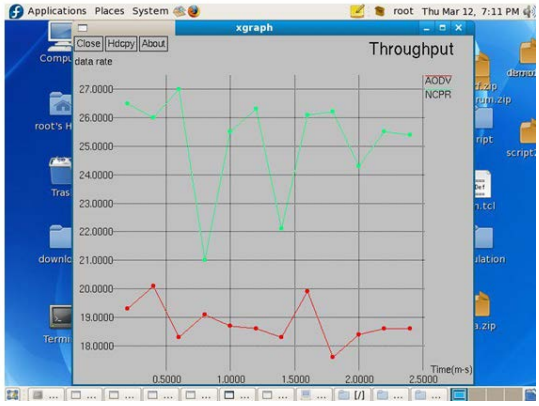

Fig. 5: Throughput graph

CONCLUSION

The control plane routing algorithm can be validated using the connectivity record of each node in MANET'S. Thereby, it allows defending against malicious node to disseminate incorrect information about their connectivity. Thus, identifiers in the nodes can be extracted and recorded by using a space efficient scheme. The protocol applied provide a more secure and efficient architecture. In pace with the increased mobility, ad hoc networks have many benefits in the near future.

REFERENCES

01. Wu, B., J. Chen, J. Wu and M. Cardei, 2007. A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks. In: Wireless Network Security. Yang, X., X.S. Shen and Z.D. Ding (Eds.). Springer US, New York, USA., ISBN: 978-0-387-28040-0, pp: 103-135.
02. Butler, K., T.R. Farley, P. McDaniel and J. Rexford, 2010. A survey of BGP security issues and solutions. Proc. IEEE, 98: 100-122.
03. Perlman, R.J., 1988. Network layer protocols with byzantine robustness. Ph.D. Thesis, Massachusetts Institute of Technology, Cambridge, Massachusetts, USA.
04. El-Defrawy, K. and G. Tsudik, 2011. ALARM: Anonymous location-aided routing in suspicious MANETs. IEEE Trans. Mobile Comput., 10: 1345-1358.
05. Alicherry, M., A.D. Keromytis and A. Stavrou, 2009. Deny-by-default distributed security policy enforcement in mobile ad hoc networks. Proceedings of the International Conference on Security and Privacy in Communication Systems, September 14-18, 2009, Athens, Greece, pp: 41-50.
06. Alicherry, M. and A.D. Keromytis, 2010. Diploma: Distributed policy enforcement architecture for MANETs. Proceedings of the 2010 4th International Conference on Network and System Security, September 1-3, 2010, IEEE, Melbourne, Australia, pp: 89-98.
07. Jia, Q., K. Sun and A. Stavrou, 2011. CapMan: Capability-based defense against multi-path Denial of Service (DoS) attacks in MANET. Proceedings of 20th International Conference on Computer Communications and Networks (ICCCN'11), July 31-August 4, 2011, IEEE, Maui, Hawaii, USA., pp: 1-6.
08. Ballani, H., Y. Chawathe, S. Ratnasamy, T. Roscoe and S. Shenker, 2005. Off by default!. Proceedings of the 4th International Workshop on Hot Topics in Networks (HotNets-IV), November 14-15, 2005, College Park, Maryland, pp: 1-6.
09. Wolf, T., 2007. A credential-based data path architecture for assurable global networking. Proceedings of the IEEE International Conference on Military Communications (MILCOM'07), October 29-31, 2007, IEEE, Orlando, Florida, USA., pp: 1-7.
10. Duffield, N.G. and F.L. Presti, 2004. Network tomography from measured end-to-end delay covariance. IEEE/ACM. Trans. Netw., 12: 978-992.
11. Tian, H. and H. Shen, 2004. Mobile agents based topology discovery algorithms and modelling. Proceedings of the 7th International Symposium on Parallel Architectures, Algorithms and Networks (ISPAN'04), May 10-12, 2004, IEEE, Hong Kong, China, pp: 502-507.

12. Chandra, R., C. Fetzer and K. Hogstedt, 2002. Adaptive topology discovery in hybrid wireless networks. Proceedings of the 1st International Conference on Ad-Hoc Networks and Wireless, September 20-21, 2002, Toronto, pp: 1-16.
13. Chasaki, D. and T. Wolf, 2009. Evaluation of path recording techniques in secure MANET. Proceedings of the 2009 IEEE International Conference on Military Communications (MILCOM'09), October 18-21, 2009, IEEE, Boston, Massachusetts, USA., pp: 1-6.