A Novel Paradigm: RIP (Reputation Index Protocol) For MANET

Kirti Patil
M Tech Student, PCST, Indore

Praveen Bhanodia
HOD, PCST Indore

Shubham Joshi
Faculty, SAIT, Indore

Abstract:
Reputation of any volatile node reflects its utility inside the MANET for performing various tasks. The reputation is the term by which we can understand the efficacy of any participating node. It's a very vital in the infrastructure less wireless network that their participating nodes perform whatever must match with their objective and perspective. When one node would like to transfer their data and operands to other nodes with means of acknowledgement based scheme than using node feedback system we can analyze one's reputation index, to find suitable among available nodes for further and hence we can establish trust between nodes or networks. The occurrence of reliability and trust coefficient can be applied in combined approach to accommodate the usefulness of reputation model. So our approach is to consider all issues and challenges for establishing reputation into common place and to propose a reputation Index Protocol that remunerate its objective.

Keywords*: Reputation, Reputation Index, trust, reliability, Selfish Index.*

I. Introduction:

A Mobile Ad-Hoc Network is a self constrained, self-configuring and resource poor network of mobile nodes connected by wireless links, this combination schematizes a random topology. The evolutions of next generation mobile ad-hoc network inquire about to provide users on demand services in a wide spectrum of large infrastructure less wireless computer network, participated by various mobile terminals (motes). The distribution points i.e. routers are free to move arbitrary and organize themselves illogically (randomly); this may cause the modification of recent topological environment and hence motes can move across the network rapidly and unpredictably. This nature of non prediction may lean the network scenario downwards and motes become vulnerable (become weak), that can be easily tampered further.

One of the primary concerns related to ad hoc networks is to provide a secure communication among mobile nodes in a hostile environment. The nature of mobile ad hoc networks poses a range of challenges to the security design. These include an open decentralized peer-to-peer architecture, a shared wireless medium and a highly dynamic topology. This last point is where the main problem for MANET security resides: the ad hoc networks can be reached very easily by users, but also by malicious attackers. If a malicious attacker reaches the network, the attacker can easily exploit or possibly even disable the mobile ad hoc network.

Similar to wired and standard wireless networks, the first line of defense in a MANET is constituted by intrusion prevention systems like cryptography and authorization. However, the implementation of these mechanisms is not always possible due to the limitations that some nodes may present. For example, if the node is a sensor, one of the constraints for its operation is the power consumption. The encryption of messages can be too energy demanding for the node to perform it without compromising its capacity.

II. Literature Survey:

The nature of mobility creates new vulnerabilities that do not exist in a fixed wired network and many of the proven security measures become ineffective. Therefore, the traditional way of protecting networks with firewalls and encryption software is no longer sufficient. For instance, if one of the nodes in the network is an unattended sensor or a personal computing device like a hand held, that node can get lost, stolen or compromised, allowing for a malicious node to obtain legitimate credentials and launch more serious attacks inside the network. This rarely happens in a wired network, but in a MANET it will be void the encryption defense. In MANET, the use of wireless links creates a very open medium that does not allow definition of clear line of defense and renders the network susceptible to attacks from passive eavesdropping to active interfering. Every node must be prepared for encountering with an adversary directly or indirectly.

Due to the momentary environment of MANET (the network is created "on the fly") and the mobility of nodes, it is not possible to designate a centralized authority. This is opposite to wired networks where the central authority can be a switch or a router, and also opposite to standard wireless networks where the central authority is the base station. This lack of a centralized authority forces the nodes to use cooperative algorithms. The decision making in many important protocols, such as routing, is collaborative. This also means that the adversaries can exploit this vulnerability for new types of attacks designed to break the cooperative algorithms.

The specific interest here is on the access to the network-layer functionalities like routing and packet forwarding. Access should be given only to well-behaving nodes and not to misbehaving nodes. A misbehaving node can be either a selfish or a malicious node. A selfish node may enjoy network services, e.g. receiving packets destined for itself but refuse to route or forward packets for others, therefore invalidating the basic collaboration premise in almost all current routing algorithms for mobile ad-hoc networks. A malicious node may seek to damage or disrupt normal network operations. Moreover, misbehaving node may act as a good network citizen for a certain time period or in certain places, but then starts to act selfishly or maliciously at other times or locations.

A Trivedi et al [1] schematized a RISM design is based on the Reputation paradigm and possesses a Semi-distributed nature. The term semi-distributed is used for the system observation which is neither restricted locally to our self nor immediately propagated it to the whole network as is the case in true distributed systems like CONFIDANT. The design has been kept very simple keeping in mind the amount of traffic already in the network and the critical amount of battery and computational power individual nodes possess. RISM system runs on every node in network

Vivek Shrivastava et al [2] proposed a reputation-based mechanism as a means of building trust among nodes. Here a node autonomously evaluates its neighboring nodes based on completion of the requested service(s). The neighbors need not be monitored in open area as in other reputation based methods. No need of exchanging of reputation information among nodes. Thus involves less overhead, and this approach does not rely on any routing protocol.

Pietro Michiardi [3] proposed a Collaborative Reputation (CORE) mechanism that also has a watchdog component for monitoring. Here the reputation value is used to make decisions about cooperation or gradual isolation of a

node. Reputation gives values are obtained by regarding nodes as requesters and providers, and comparing the expected result to the actually obtained result of a request. This method gives more importance to the past behavior and hence tolerable to sporadically bad behavior, e.g. battery failure. But the assumption that past behavior to be indicative of the future behavior may make the nodes to build up credit and then start behaving selfishly.

Sonja Buchegger et al [4] described evidence from direct experiences and recommendations are collected. Trust relationships are established between nodes based on collected evidence and trust decisions are made based on these relationships. There are four interdependent modules; (a) monitor, (b) reputation system, (c) path manager and (d) trust manager. Monitor collects evidence by monitoring the transmission of a neighbor after forwarding a packet to the neighbor. It then reports to the reputation system only if the collected evidence represents a malicious behavior. Reputation system changes the rating for a node if the evidence collected for malicious behavior exceeds the predefined threshold value. Then, path manager makes a decision to delete the malicious node from the path. Trust manager is responsible for forwarding and receiving recommendations to and from trustworthy nodes. But this approach does not talk much about isolating the misbehaving nodes from the network.

Tiranuch Anantvalee et al [5] described, a new type of node called as suspicious node besides cooperative nodes and selfish nodes, some actions will be taken to encourage the suspicious nodes to cooperate properly after further investigation. They introduce the use of a state model to decide what to do or respond to nodes in each state. In addition to a timing period for controlling when the reputation should be updated, a timeout for each state is introduced.

Fei Wang [6] et al described the Cooperative On-Demand Secure Route (COSR), is a novel secure source route protocol which takes action against malicious and selfish behaviors. COSR measures node reputation (NR) and route reputation (RR) by contribution, Capability of Forwarding (CoF) and RR is used to balance load and to avoid hot point. In the COSR, nodes' reputation depends on the information from Physical layer, Media Access Control (MAC) layer, and Network layer, and it can be computed by node's CoF, history action, and recommendation.

Sangheetaa Sukumarn et al [7] introduced CoF (Capability of Forwarding) that denotes the capability of forwarding packets of a certain node. As the information of CoF is provided by its owner, malicious node might cheat others by false data. To avoid the emergence of such malicious behavior, COSR takes strategies: 1. Discounting where COSR uses nodes' reputation to discount those providing CoF data. 2. Punishment. Where once COSR finds that any node provided a false CoF, it will punish such node through reducing its reputation level. But the authors have not clearly specified how COSR will decide whether the advertised information is false or not.

R. Sameh Zakhary [8] described a reputation model based on Eigen vector based degree centrality. Here each node collects information about its neighbor by direct monitoring as well as from other neighbors. Trust is built based on these centralities. Nodes with higher centrality have higher probability of getting in contact with other nodes. Second hand information is collected only from those neighbors with high centrality not from all the neighbors.

III. Problem Domain: The vulnerability index may become insecure for participating nodes, when they move across unpredictable environment. The value of reliability index reduced when the node denies ones' packet to forward further. This reduction can foster the attackers to move forward and to promote malfunction and get the node down. This can further reduce the node cooperation hence the occurrence of selfish index can increase and thus the overall reputation index can be decrease. The mitigation from these errors are essential to facilitate the network a hassle free routing.

IV. Proposed work:

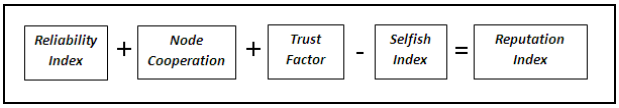

Figure1: Concept Diagram of Reputation Index Generation across MANET

When one node would like to transfer their data and operands to other nodes with means of acknowledgement based scheme than using node feedback system we can analyze one's reputation index, to find suitable among available nodes for further and hence we can establish trust between nodes or networks. Our proposed work states that the conjunction of Reliability Index, Node Cooperation, trust factor and disjunction of Selfish index from the integration of these logical values. Thus the reputation among participating nodes can be assessed and the applied induction from this can be measured by node cooperation index. The threshold value of node cooperation can be termed as reputation across nodes, hence the data packets can be safe and secure and packet drop attack can be mitigated.

V. Conclusion & Future Scope:

The emphasis is given to calculate the reputation values of the nodes using conjunction of Reliability Index, Node cooperation Index, Trust Factor and the disjunction of selfish index. This formula simplifies the ideology towards calculating reputation across MANET. Any node is supposed to maintain a good reputation value in order to receive network services. Only by forwarding other nodes' packets a node can maintain a high reputation value. Thus behaving selfish will not help them. This encourages nodes to be cooperative. This approach has the clear advantage of simplicity, ability to get a trustworthy route etc. The reputation index calculation is the prime parameter to achieve trust across MANET. So, the proposed work may develop a revolutionary concept in ad hoc networks to maintain security, integrity and robustness among participating nodes. The scope of this work is to extend further the reputation index protocol that can ensure the end to end communication in public domains.

References

[1]. Animesh K. Trivedi, Rishi Kapoor, Rajan Arora, Sudip Sanyal and Sugata Sanya, "RISM Reputation Based Intrusion Detection System for Mobile Ad hoc Networks" Available from link: profile.iiita.ac.in/aktrivedi_b03/rism.pdf.

[2]. M. Tamer Refaei, Vivek Srivastava, Luiz De Silva, Mohamed Eltoweissy, "A Reputation based Mechanism for Isolating Selfish Nodes in Ad Hoc Networks", Proceedings of the Second Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services (MobiQuitous'05) , 2005

[3]. Pietro Michiardi and Refik Molva, "CORE: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," Sixth IFIP conference on security communications, and multimedia (CMS 2002), Portoroz, Slovenia, 2002.

[4]. Buchegger, Sonja; Le Boudec, Jean-Yves, "Performance Analysis of CONFIDANT Protocol: Cooperation of Nodes - Fairness in Dynamic Ad-Hoc Networks," Proceedings of IEEE/ACM

Workshop on Mobile Ad Hoc Networking and Computing (MobiHOC). IEEE, June 2002.

[5]. Tiranuch Anantvalee, Jie Wu: "Reputation-Based System for Encouraging the Cooperation of Nodes in Mobile Ad Hoc Networks", Proceedings of International conference of Communications, pp 3383-3388, 2007.

[6]. Fei Wang. Furong Wang, Benxiong Huang, Laurence T. Yang, "COSR: a reputation-based secure route protocol in MANET" in Journal EURASIP Journal on Wireless Communications and Networking - Special issue on multimedia communications over next generation wireless networks archive Volume 2010, pp. 1-11, January 2010.

[7] Sangheetaa Sukumarn Venkatesh Jaganathan and Arun Korath "Reputation based Dynamic Source Routing Protocol for MANET", *International Journal of Computer Applications (0975 – 888) Volume 47– No.4, June 2012.*

[8]. Sameh R. Zakhary and Milena Radenkovic ,"Reputation based security protocol for MANETs in highly mobile disconnection-prone environments" in International conference on Wireless On-demand Network Systems and Services (WONS), PP. 161 – 167, Feb. 2010.