Reputation-Based Security Protocol for MANETs in Highly Mobile Disconnection-Prone Environments

Sameh R. Zakhary
email: itxsraz@nottingham.ac.uk

Milena Radenkovic
email: mvr@cs.nott.ac.uk

School of Computer Science & IT
University of Nottingham
Nottingham, NG8 1BB, UK

Abstract

This paper is concerned with fully distributed reputation-based mechanisms that improve security in MANETS. We introduce a number of optimisations to the current reputation schemes used in MANETs such as selective deviation tests and adaptive expiration timer that aim to deal with congestion and quick convergence. We use two different centrality measures for evaluation of the individual trust claims and resolving the aggregated ones. We design and build our prototype over AODV and test it in the NS-2 in the presence of variable black hole attacks in highly mobile and sparse networks. Our results show that we achieve increased throughput while delay and jitter decrease and converge to AODV.

Keywords: MANET, reputation, trust, routing

I. INTRODUCTION

There has been a proliferation of interest in ad hoc network security that due to potentially high mobility of nodes and lack of common infrastructure render conventional security solutions dysfunctional due to their dependence on centralized authority. A wide range of fully distributed reputation-based security protocols for ad hoc networks have been proposed but usually tested in relatively low mobility or even semi static scenarios (i.e. long pause time between node movement and slow node speed [3][4][18]).

This paper is concerned with the design, implementation and evaluation of a reputation-based self organized protocol that is specifically targeted for highly mobile and sparse environments. Our protocol follows distributed reputation guidelines given in [1] and considers two types of Centralities to improve on the reputation convergence and faster isolation of malicious nodes. We incorporate our protocol within AODV and perform extensive simulations a number of scenarios characterized by high node mobility (speed 20 m/s), short pause time (1 second) and highly sparse network in order to evaluate each of the design choices of our system. We focus on a single and multiple black hole attacks [2] but our design principles and results are applicable to a wider range of attacks such as gray hole attacks. The rest of the paper is organised as follows. Section 2 gives brief review of the related work. Section 3 describes our proposed protocol. Section 4 gives our results and Section 5 concludes and identifies future work.

II. RELATED WORK

Distributed reputation has been used in both MANETs and P2P environments. CORE [6] proposed a watchdog for monitoring and isolating selfish nodes based on a subjective, indirect and functional reputation. CONFIDENT [7] proposed using an adaptive Bayesian reputation and trust system where nodes monitor their neighbourhood and detect several kinds of misbehaviour. SCAN [4] proposed a network layer security protocol that relies on collaborative localised voting to convict malicious nodes and using asymmetric cryptography to protect the token of normal nodes. In the peer-to-Peer file-sharing networks, reputation has been used to reflect the ratings of different users and distributed Eigen-Vector has been proposed to calculate trust in a distributed Peer-to-Peer environment. Ref. [8], proposed EigenTrust algorithm that assigned each peer a unique global trust value, based on the peer's history of uploads. EigenTrust used 1 or -1 to represent user's satisfaction or dissatisfaction about the download transaction respectively. In our model, node's reputation is classified to not only good or bad but we classify nodes into multiple zone that enable higher details and better decision making depending on the required services such as packet forward or Topology discovery as described below. Other researches attempted to provide routing layer solutions to black hole attacks, with techniques to identify and isolate these nodes as in [9][10]. [9] proposed that a node communicates with one extra node while [10] considered static sensor networks which are not similar to MANET conditions. Ref. [11] proposed a solution to collaborative black hole attack using next hop information validation but showed no results or detailed analysis.

III. OUR REPUTATION-BASED FULLY DISTRIBUTED PROTOCOL FOR HIGHLY MOBILE AND SPARSE MANETS

A Functional Overview

Our reputation based protocol integrates four main features of distributed reputation systems proposed in [1] and shows how they can be extended by utilising different kinds of centrality of nodes even in highly mobile and disconnection-prone scenarios. Each node in a MANET collects reputation information, through direct observation of its neighbours (subjective observation) and gathers indirect (second hand) reputations from other nods. In addition to using historical observations, our protocol uses reputation discounting to ensure that old reputations will fade away giving more chance for nodes to reclaim their reputation by consistently behaving in a cooperative manner. We use secondary response to retaliate against any neighbour who originally had a bad reputation that then got reclaimed, if this neighbour shows early signs of misbehaver afterwards, to avoid reputation discounting firing-back. We employ reputation noise detection and cancellation, deviation test and secondary response that are specifically tailored for our highly challenged environment in order to increase the accuracy and reliability of the reputation resolution

We consider two kinds of Centrality: Eigen vector and degree centrality in order to elect the most influential nodes to assist in the role of helping other nodes to build their trust into other less popular nodes in the network and act as community leaders.. Nodes with higher centrality have higher probability of getting in contact with many other nodes than nodes with low centrality.

We identify the nodes that have both high centrality and high reputation as preferred sources for indirect reputation. This becomes even more important in high-mobility and sparse networks, as nodes often have few connections –if any- at any point in time, these connections are frequently changing which causes more uncertainty. We argue that nodes with higher centrality and higher reputation are prime nodes to give highly trusted opinions about other nodes in MANET in a self-organized manner. We use centrality of ego networks for each node to obtain localized view of its neighbourhood to allow fast reputation convergence and subsequently higher throughput

Figure 1 shows an example of how we use Eigen-Vector reputation-based centrality to influence nodes decision about the reputation of other nodes and the importance of indirect-reputation exchanged between nodes. Both centrality of the reporting nodes and indirect-reputation are key to quick isolation of the malicious nodes and convergence of reputation across all the nodes.

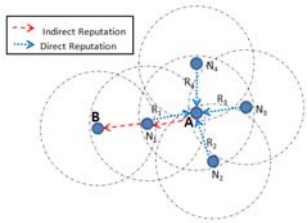

Figure 1: Eigen-Vector Reputation-Based Centrality.

In Fig. 1, node A is the observed node and each of its neighbours has a direct reputation measure for it as R1 to R4 respectively. Node B, that is not directly connected to node A, receives R1-R4 reputation observations about Node A. By applying the Eigen-Vector reputation-based centrality, as discussed in section B below, node B will have a centrality measure based on all Node A's neighbouring nodes reputation evaluation of that node. Using this technique makes Node B immune against an attack where one node would collude with multiple other nodes to provide false indirect reputation about node A, as indirect reputation reported by N1-N4 is subject to selective deviation test that is described in the section B.

When we resolve node's reputation as a function of its centrality characteristics, we classify it as high, medium or low centrality.

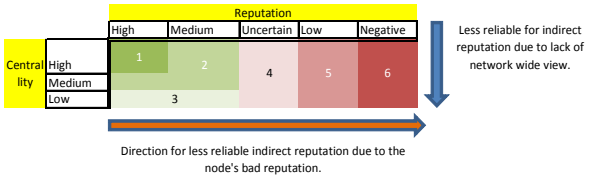

Figure 2: Self-Organized node selection for indirect-reputation information.

Fig. 2 shows how we classify the observed nodes into zones based on their reputation and centrality. Nodes falling into zone 1 are highly trusted nodes that also have wider view of the network. Nodes that are classified as belonging to that zone have privileges such as higher watchdog expiration time and they are exempted from the deviation tests on their reported indirect-reputation, low or no discounting factor, and high Reputation-Record expiration time. On the other hand, nodes falling into zone 6 are classified as miss-behaving nodes, so their reported indirect-reputation is rejected. Nodes falling in zones between 1 and 6 would have different levels of acceptance and the different parameters would be adjusted to reflect their current zone. Nodes classification can change over time. This can be a result of a good reputation node that started to behave maliciously and hence become less trusted and fall to a less favourable zone. This technique allows the network to evolve into a multiple clusters of different trustworthiness levels. These different levels of trust-worthiness allow higher layer applications to limit their interaction only to one selected zone vs. any other zone.

B Architectural Overview

Fig. 3 shows the interaction between the key components of our reputation model in order to provide automatic and autonomous routing decisions to the under-laying routing protocol based on the available neighbours' reputations.

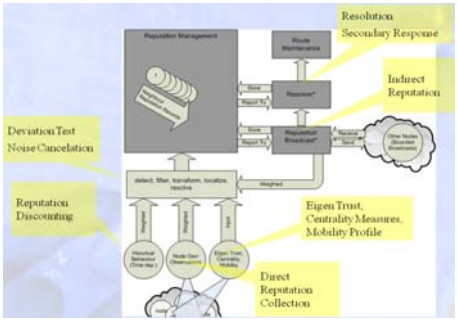

Figure 3: Reputation system model.

Reputation Management is the main entity responsible for storing and retrieving all the node's neighbours' reputation records. It orchestrates the operations of the other components and act as the concentration point for all the events taking place inside the system. *Neighbour Reputation Record* is the entity representing reputation observation for one of the neighbours. Each node holds N neighbour reputation records where N can be determined by the node's memory capacity, CPU power for maintenance to update these records and other resource constraints. Nodes with higher reputation and centrality should hold enough reputation records about other nodes in order to provide adequate coverage of the nodes in its own area. Node recycles these records using expiration time to balance the different overheads with the need to have enough reputation about different neighbours.

Reputation Broadcast is the entity responsible for receiving indirect reputation from neighbours. It performs a **selective deviation test** to ensure the unity of view with the receiving node point of view. Traditional Deviation Test as presented in [1], requires each node to compare received indirect reputation with its own direct reputation for a given neighbour and reject any indirect reputation that deviate by a certain value Δ (the deviation threshold). In our Selective Deviation Test, the receiving node (a) attempts to calculate the reputation of its neighbour node (j). Node (a) first checks the reputation of the indirect reputation information source node (i). R_{ai} is the reputation held by node (a) about node (i). If the reputation R_{ai} > (threshold) then R_{ij} is trusted without further tests. This enables fast reputation convergence which is critical in our challenged scenarios where

nodes don't get enough time to observe the reputation of other nodes. At the same time, node (*a*) uncertainty with respect to node (*j*) decreases as a result of trusted node (*i*). We follow the same definition of uncertainty as used by Feng et al. in [14].

Reputation Detect, Filter, Transform and Localize: The calculation of the direct reputations was inspired by the Eigen Trust algorithm presented in [8]. Our algorithm calculates a global consistent reputation value at each node for all its neighbours and then resolves the reputation using direct and indirect (second hand) reputation information. Each node calculates the Eigenvector centrality of its neighbours in order to reflect on each neighbour reputation and the level of confidence in this neighbour reported indirect reputation. x_i denote the score of the i^{th} node. Let $A_{i,j}$ be the adjacency matrix of the network. $A_{i,j}$ is originally defined in Eigen-Vector Centrality as $A_{i,j} = 1$ if the i^{th} node is adjacent to the j^{th} node, and $A_{i,j} = 0$ otherwise. In our model, $A_{i,j} = s$, where s is the wireless signal strength from the i^{th} node to its neighbour j^{th} node, and $A_{i,j} = 0$ if the i and j are not neighbours. For the i^{th} node (the observed node), the centrality score is proportional to the sum of the scores of all nodes which are connected to it. Hence:

$$x_i = \frac{1}{\lambda} \sum_{j \in M(i)} x_j = \frac{1}{\lambda} \sum_{j=1}^{N} A_{i,j} x_j$$

Where M(i) is the set of nodes that are connected to the i^{th} node, N is the total number of nodes and λ is a constant. For the purpose of our reputation schema we use connectivity instead of transaction. This connectivity takes place when the node either receives or requests a forward of a message from that neighbour. In our distributed network environment, each node marks its experience when it comes into contact (i.e. becomes connected) with another neighbour. Periodically, each node will evaluate its connectivity experience with each of its direct neighbours and gives it a rating and vice versa. Node *i* calculate the percentage of packets originating from *i* that were forwarded by node *j* over the total number of packets offered to node *j*, *frwd(i,j)*, and the percentage of packets that were expired (i.e. packets that were originating or forwarded by node *i* to node *j* but they were not subsequently forwarded by node *j*) over the total number of packets offered to node *j, expr(i,j)*.

$$S_{ij} = frwd(i,j) - expr(i,j)$$

Where S_{ij} is the recent satisfaction index for node *i* about node *j*. S_{ij} would be then weighted into the direct reputation of node *j*:

$$R_{ij} = R_{ij\text{-}prev} * W_{history} + S_{ij} * (1\text{-}W_{history}).$$

If no connectivity between *i* and *j* takes place, R_{ij} is discounted instead. We define $\max_t$ to be the maximum observation of R_{ij} over time. R_{ij} is normalized as:

$$R_{ij} = R_{ij} / \max_t (R_{ij})$$

Variable/Adaptive Observation Expiration Time is the time that a node waits for its direct neighbour to perform the requested function before a watchdog times-out and penalize that neighbour for its failure (i.e. forward the packet). Nodes are able to monitor their neighbours' behaviour by utilizing the shared nature of the wireless medium and constantly overhearing its neighbours' traffic. We propose a **per neighbour/adaptive expiration technique** that allows a node to adjust depending on its neighbour reputation and network conditions. For trusted neighbours, the observation expiration time would be higher than for non-trusted neighbours. Network or Node Congestion, if detected by an observing node, it would increase its expiration time accordingly. This would decrease the number of false positive and enable the protocol to selectively adjustable in responses to different network conditions.

Resolver is responsible for doing the actual calculation of the neighbour final reputation (called resolved reputation) by combining direct and indirect reputation and performing Reputation Noise Cancellation. As packets might get dropped accidently by nodes due to other network conditions such as congestion, interference which doesn't constitute malicious behaviour, we have included an adaptive threshold measure that is adjusted depending on the neighbour node movement profile and the link quality between the observing node and its neighbours. Depending on the node own knowledge about the medium quality reported by the node's physical layer, the node is able to adjust the threshold of acceptable silent error level from that neighbour. If the node experiences a packet loss from its neighbour below this threshold, it considers that loss as a noise and subsequently ignores the lost packets. If the losses were above the noise threshold level, the node will start reacting to these events accordingly.

R*oute* M*aintenance* is being called when the Resolver detect that a certain neighbour reputation has fallen below a certain threshold. The "Route Maintenance" entity is responsible for breaking all the routes going through this neighbour and initiates a new replacement route search as needed. In our implementation using AODV, the "Route Maintenance" entity sets the route to a special mode called "Local Route Repair" as described in [16]. This special route mode would enable queuing packets going out on the route until an alternative route is established if possible, else all the packet queued are dropped and a route error (RERR) message is sent to the neighbour nodes.

Different components of our proposed model rely on a number of observed parameters that affect neighbour specific or node wide parameters in a complete state-machine for each node as shown in Fig 4 below.

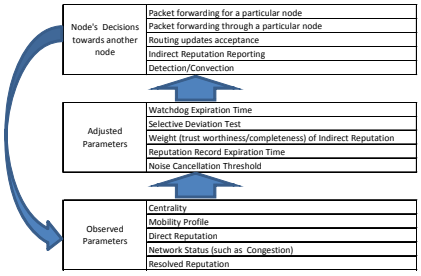

Figure 4: Reputation system parameters.

IV. EARLY PROTOTYPE IMPLEMENTAION AND RESULTS

We have performed a number of experiments in highly mobile and disconnected topologies where network experienced frequent neighbourhood changes and lower route stability. We have integrated our reputation-based protocol with AODV. Our simulation scenarios included 20 mobile ad-hoc nodes randomly

moving in 750m X 750m area where the simulation time was 500 second and the mobile node wireless range was 250m, our nodes' speed was 20 m/s, and pause time was 1 sec that is significantly very short pause time compared to 300 sec in [17]. The percentage of black hole nodes that we used is much higher than in other test scenarios found in [17] were the scenarios used up to a maximum of 20% black hole nodes.

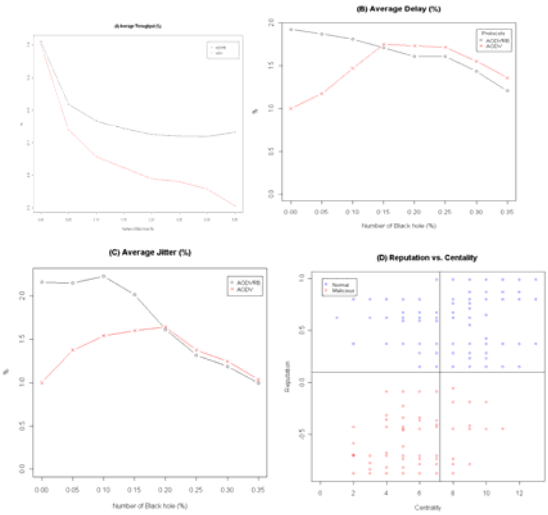

Figure 5: (a) Average Throughput, (b) Average Delay, and (c) Average Jitter with various number of black hole nodes.

Fig. 5 (a), shows that the network throughput for our reputation-based protocol gracefully falls as the number of malicious nodes increase but it remains bounded above 70% (benchmark is AODV throughput without black hole attack). At the same time, AODV with a black hole is continuing to drop below 50%. Fig. 5 (b), shows that while the average data packet delay (Delay = arrival time – send time, Averaged over all the data packets sent during the scenario) is high in AODV with reputation compared to AODV with no reputation, it does converge to AODV as the number of malicious nodes approach 15%. This can be attributed to the speed by which the malicious nodes are identified and isolated as their number increase due to the higher probability that they will come across normal node, this helps to quickly resolve the reputation of malicious nodes and decrease uncertainty as explained in [14]. As the number of malicious nodes increase above 20%, the Average delay becomes lower than AODV without reputation. Fig. 5 (c), shows the average data packet Jitter comparison between AODV and AODV with Reputation. It shows that AODVRB has considerably higher Jitter when the percentage of the black hole nodes is below 15% compared to AODV without reputation. This can be explained as the node has higher probability of meeting new nodes with no prior reputation; the node will be reluctant to switch to any of these new neighbours even though they might have been able to offer shorter paths with less delay and jitter. As the number of black hole nodes approach 20% of the total number of nodes, AODVRB does converge fast to AODV. This can be attributed to the fact that the network was able to quickly identify and isolate malicious nodes as the black hole nodes have higher probability of meeting good nodes. And the probability of meeting new unknown node decreases. Fig. 5 (d), shows the distribution of reputation and centrality of normal and malicious node. Our observations show that higher centrality normal nodes advance in their reputation faster than lower centrality normal nodes. At the same time, lower centrality malicious nodes are slower to isolate than other malicious nodes that have higher centrality.

V. CONCLUSION AND FUTURE WORK

Our proposed reputation framework relies on centrality and mobility as two key parameters to drive the system to a more stable state in highly mobile, sparse and disconnected environments. We discuss how we integrate two kinds of centrality in our reputation-based protocol and propose a number of optimisations for more efficient node monitoring and trust resolution such as selective deviation test and adaptive expiration timer. Our early prototype implementation over AODV confirms and extends the results published in [3][4][5]. The results presented in this paper show that the throughput remains above 70% in the presence of the increasing number of blackhole nodes while the jitter and delay decrease and are below AODV. We also discuss the impact the distribution of centrality and reputation of our nodes has on the time needed to isolate malicious nodes.

Our subsequent work will focus on studying the impact of centrality and configuration parameters on the protocol performance in relation to network throughput, network delay, network jitter and the protocol detection ratio. We will investigate the response of the reputation protocol under the same high-mobility conditions and subject to collaborative black hole and gray hole attacks.

REFERENCES

[1]S. Buchegger, "Reputation Systems for Self-Organized Networks: Lessons Learned," In IEEE Technology and Society Magazine, Toward Fourth Generation Wireless, March 2008., pp. 1-10.

[2]J. Ruiz, et al, "Black Hole Attack Injection in Ad hoc Networks," DSN2008, International Conference on Dependable Systems and Networks. Anchorage, Alaska, June 24-27 2008, pp. G34-G35.

[3] Sonja Buchegger and Jean-Yves Le Boudec. Performance Analysis of the CONFIDANT Protocol: Cooperation Of Nodes — Fairness In Dynamic Ad-hoc NeTworks. In *Proc. of IEEE/ACM MobiHOC*, 2002. IEEE.

[4]H. Yang, et al, "SCAN: Self-Organized Network-Layer Security in Mobile Ad Hoc Networks," IEEE Network, vol. 24, 2006, pp. 1-13.

[5]A. Dadhich, "A Distributed Cooperative Approach To Improve Detection And Removal Of Misbehaving MANET Nodes", COMSWARE, 2008, pp728 - 735

[6]P. Michiardi and R. Molva, "CORE: A Collaborative Reputation Mechanism to enforce node cooperation in Mobile Ad hoc Networks", Proc. IFIP CMS, 2002.

[7]S. Buchegger and J.L. Boudec, "A robust reputation system for peer-to-peer and mobile ad-hoc networks", proc. of P2PEcon, 2004..

[8]M.T. Schlosser, "The EigenTrust Algorithm for Reputation Management in P2P Networks," ReCALL, 2003.

[9]H. Deng, W. Li, and D. P, "Routing Security in Wireless Ad Hoc Network", IEEE Communications Magzine, vol 40, 2002.

[10]U. Jian Yin, Sanjay Kumar Madria, "A Hierarchical Secure Routing Protocol against Black Hole Attacks in Sensor Networks," IEEE-SUTC, vol. 1, 2006.

[11]S. Ramaswamy et al., "Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks", ICWN'03, USA 2003..

[12] S. Ramaswamy et al, "Simulation Study of Multiple Black Holes Attack on Mobile Ad Hoc Networks," ICWN'05, 2005, pp. 595-604.

[14]F. Li, J. Wu, and B. Raton, "Mobility Reduces Uncertainty in MANETs", Proc. of IEEE INFOCOM, May 2007.

[15]E. Daly and M. Haahr, "Social Network Analysis for Routing in Disconnected Delay-Tolerant MANETs," Source, 2007, pp. 32-40.

[16]C.E. Perkins and E.M. Royer, "Ad-hoc on-demand distance vector routing,", In proc. of 2nd IEEE Workshop on Mobile Wireless Networks, 1999.

[17]C.W. Yu, et al, Distributed and Cooperative Black Hole Node Detection and Elimination Mechanism for Ad Hoc Networks, Springer 2009.

[18] A. Dadhich, et al. "A Distributed Cooperative Approach To Improve Detection And Removal Of Misbehaving MANET Nodes", COMSWARE, 2008.