International Journal of Information & Computation Technology.
ISSN 0974-2239 Volume 4, Number 8 (2014), pp. 829-834

http://www. irphouse.com

Trust Based Detection and Elimination of Malicious Nodes

S Kaushik[1], Steve Jose Febin[2], R Alakar Srinivasan[3] and N Maalolan[3]

Electronics and Communication Engineering Department
Sri Sivasubramaniya Nadar College of Engineering
Kalavakkam, Chennai-603110 INDIA

ABSTRACT

In general Mobile Ad-Hoc Networks (MANETs) employ conventional routing algorithms like AD-Hoc On Demand Distance Vector (AODV) routing to forward data. But these algorithms cannot be used effectively in a network environment where the number of malicious nodes is high. This scenario causes high delay and loss of data. To detect and eliminate such nodes this paper proposes a unique trust based routing algorithm where the next hop forward node is selected based on the ability of a node to deliver data. This ability is numerically quantified as trust rating and is used to compare various nodes based on this parameter before forwarding data to it. Hence nodes which have good forwarding interactions in the past would have higher trust rating compared to others and hence is preferred as the forwarding node in the future. This in-turn eliminates or isolates the malicious nodes, due to its lower trust rating, hence improving the efficiency of the network.

Keywords- component; formatting; Trust management; MANETs; (key words)

1. INTRODUCTION

Mobile Ad-hoc networks are networks with no fixed infrastructure and peer to peer type network. Furthermore, mobility of the nodes in the network makes it difficult to design and provide security. Traditional routing methods in Ad-Hoc networks involve data transmission from source to destination through various other nodes. The intermediate nodes are responsible for forwarding data in such a way that it would reach the destination. If the intermediate node does not forward the data or hinders it from reaching the intended destination, such a node is called a malicious node. An attack where the malicious node intentionally drops the packet is called a Black Hole attack. Such an attack would effectively cripple the network if left unattended. The existing detection methods involve receiving acknowledgement to verify if the data

has been transferred successfully by a node. But this is done for only the duration of the current data transfer and during the subsequent data transfer the malicious node is again active disrupting data transfer.

This paper introduces a reputation based detection and elimination of black hole nodes where every node is given a rating based on its behaviour in the network. If the node behaves in a malicious way then it receives a lower rating and while a trusted node receives a higher rating. Based on these ratings a node would decide the next node to transmit the data to.

2. Network Assumptions

2.1 Scenario

The scenario this paper is concerned with is a network in where highly mobile nodes are present and data is transmitted in store and forward method. We adopt a unicast method instead of multicasting to reduce the overhead of the presence of redundant data in the network.

Though multicasting improves data delivery probability it might not be suitable for networks with low bandwidth availability.

2.2 Node Specifications

Each node is assumed to be of similar capabilities and each is also assumed to contain a reliable GPS system which is able to detect the direction of motion of the node and also its velocity. Each node is also assigned a unique ID and a set of public/private keys for data encryption and decryption.

2.3 Attack Model

The network is realized by considering benign, selfish and malicious nodes. It is assumed that the network employs a suitable key management scheme employing any of the traditional cryptographic methods to protect the data integrity as it passes through intermediate nodes. Collusion attacks are also addressed by our model but not explained as it is beyond the scope of this paper. Collusion attacks are those attacks where malicious nodes work together to report a false trust value to another node.

3. Trust Management System

The objective of the trust model is to numerically quantize the trustworthiness of a node to deliver data. This is achieved in our trust model which mathematically calculates the trustable property of various nodes in the network. Every node in the network contains a table of trust value of every other node in the network. Initially all nodes in the network are assigned a Base Trust Rating (BR). This rating would then increase or decrease depending on the behavior of the node as time progresses. Every node in the network contains a routing table against which the trust rating is given for each node. Hence whenever node A forwards the data to node B the trust value of node B stored in the routing table of node A is varied.

Now when a node starts behaving maliciously or selfishly the trust value of the respective node would reduce with each interaction the node has with other nodes. But if it is not interacting with any other node for some time it would still retain its trust value. Also a selfish node avoiding other nodes for forwarding purposes would also retain its trust rating.

Consider the case of six nodes S, A, B, C, D, M where the trust value is in the order of S<A<B<C<D where S and D are source and destination nodes and also only consecutive nodes are in the range of each other. Also node M is a malicious node. As the trust value of A is greater than the trust value of S, the source node S forwards data appended with its address to the node A. Node S also notes the time the data was sent (T_I), and the trust value of node A. Now the node A has two choices that is to forward the data to either node M or node B. But M being a malicious/selfish node the following two cases can occur.

Case 1: Node A forwards data to Node M

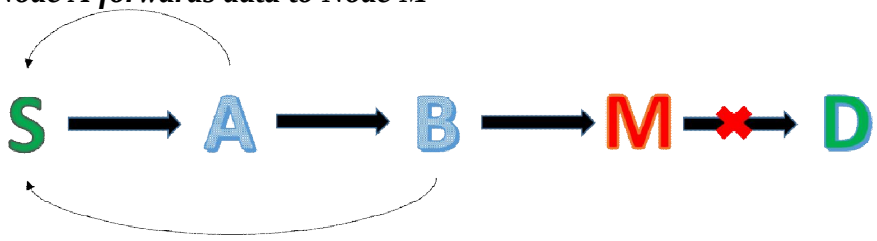

Figure 1. *Malicious node interaction*

This occurs only at the initial phase of network interaction as the trust value of the malicious node is not yet low enough for it to be detected as a malicious node. With the assumption that adequate encryption techniques are used we can safely say that Node M has only three options. Either forward data to some incompetent node, or drop the packet or forward to a competent node itself. In both the first cases the malicious/Selfish node would be easily identified when the Acknowledgement packet (ACK) arrives from incompetent node or when no ACK arrives. When the ACK doesn't come from D within a certain time called Threshold time (T_{TH}) the node S decides that node B has made a mistake in forwarding and the message needs to be retransmitted.

Case 2: Node B forwards data to Node C

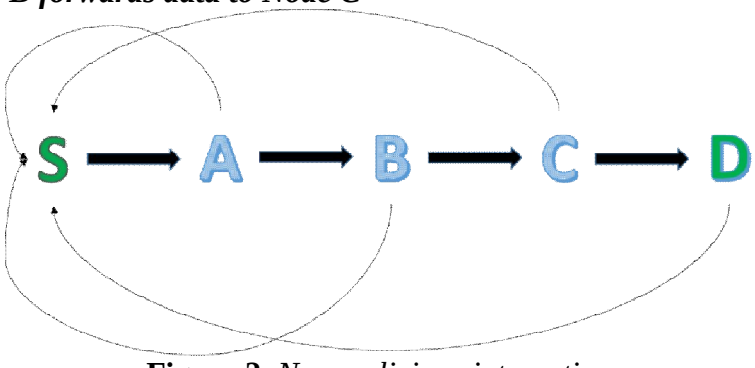

Figure 2. *Non malicious interaction*

The node B forwards the data to node C which has a higher trust value. The node C immediately sends an acknowledgement packet (ACK), its trust value to node S along with its own unique signature in encrypted form. When node S receives the ACK and it notes the time of arrival (T_A) sent along with it and calculates the time taken for the packet to be forwarded by the node (T_D).

$T_{D=}T_A$-T_I

Also node S checks if the Transfer value of the node B is better than or at least equal to node A. If not then the node has simply forwarded the data to node which has a lower probability of delivering the data than itself. Hence the trust value of node A would be reduced. Also if the ACK doesn't arrive at S then it means the node B has not forwarded the data or lost the data which in either case means the node A is incompetent to deliver the data and hence its trust value would be reduced. In both the above cases the node S would then search for some other node to transmit data. However if the data is received by B successfully and it's trust value is greater than A as in this case S would then decide that A is a trustworthy node and forwards data reliably and hence increases the trust value of the node A in its routing table according to the formula specified in the formulae section. The same process continues when B transmits to C and when C finally transmits to D

4. Equations

$$T_{AB}^{(new)} = T_{AB}^{(old)} + \frac{BR}{PDR} * (T_{TH} - T_D)$$

The equation formed numerically quantifies the trust levels of other nodes in the network. For example if the time taken by a node to deliver data is more than the threshold time (T_{TH}) the second part of the expression becomes negative and hence the trust rating of the node reduces. If the data is delivered within the threshold time then the expression is positive and the trust rating of the node is increased. Hence as a node's trust value decreases the node is slowly less preferred to forward data to and slowly it is excluded from the network.

5. Graph

As shown in the graphs fig 3 and fig 4 the proposed trust model performs better than the Ad-Hoc On Demand Vector (AODV) Protocol. In the fig 3 initially AODV protocol outperforms the proposed trust model because the process of trust calculations is acknowledgement based the overhead is high causing high delay. But as the number of the malicious nodes increases the trust model outperforms the AODV showing that the proposed model is able to eliminate the malicious nodes and is able to reduce delays due to them.

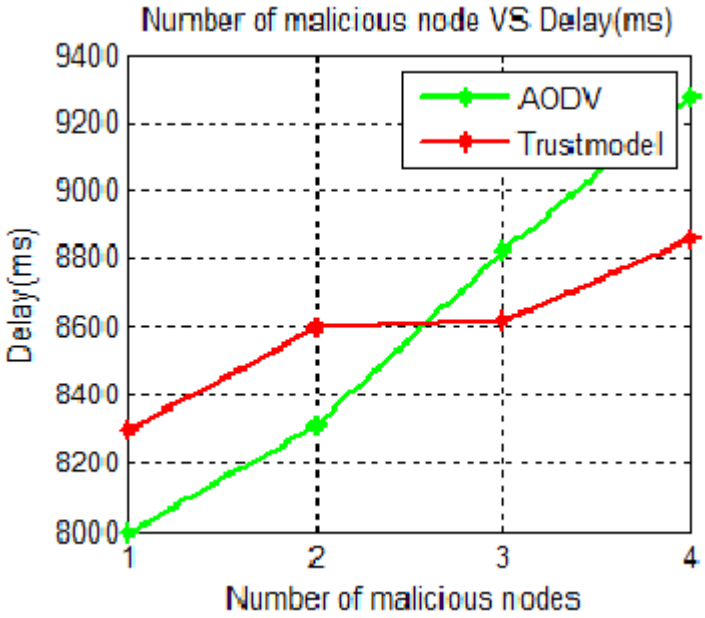

Figure 3. Number of malicious nodes VS Delay

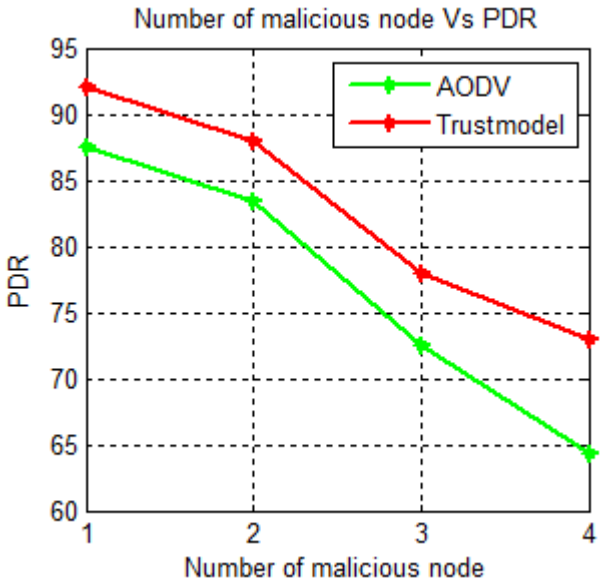

Figure 2. Number of malicious node Vs PDR

6. CONCLUSIONS

This paper has focused mainly in detection and elimination of malicious nodes. We have also been able to mathematically model the trust system in such a way to reduce the effect of malicious nodes in the network. In addition, we will integrate this idea with a novel key management scheme which is able to further secure the data than the

existing key management schemes. This key management scheme would be able to act proactively protecting the data integrity.

7. REFERENCES

[1] J. Burgess, B. Gallagher, D. Jensen, B.N. Levine, Maxprop: routing for vehicle-based disruption-tolerant networking, in: Proceedings of INFOCOM'06, 2006, pp. 1–11.

[2] V. Balakrishnan, V. Varadharajan, P. Lucs, U.K. Tupakula, Trust enhanced secure mobile ad hoc network routing, in: Proceedings of AINAW'07, Canada, 2007, pp. 27–33.

[3] C. Boldrini, M. Conti, A. Passarella, Exploiting users' social relations to forward data in opportunistic networks: the HiBOp solution, Elsevier Pervasive and Mobile Computing 4 (5) (2008) 633–657.

[4] Wang Boa, Huang Chuanhea, Li Layuanb, Yang Wenzhonga, Trust-based minimum cost opportunistic routing for Ad hoc networks, in: Elsiever Journal of Systems and Software Volume 84, Issue 12, December 2011, Pages 2107–2122

[5] Na Li, Sajal K. Das, A trust-based framework for data forwarding in opportunistic networks, Elsiever Ad Hoc Networks, Volume 11, Issue 4, June 2013, Pages 1497–1509

[6] Jason LeBrun, Chen-Nee Chuah, Dipak Ghosal, Michael Zhang, Knowledge-Based Opportunistic Forwarding in Vehicular Wireless Ad Hoc Networks, Vehicular Technology Conference, 2005. VTC 2005-Spring. 2005 IEEE 61st (Volume:4) 2289 - 2293

[7] Y.L. Sun, Z. Han, W. Yu, K.J.R. Liu, A trust evaluation framework in distributed networks: vulnerability analysis and defense against attacks, in: Proceedings of INFOCOM'06, 2006, pp. 1–13.

[8] A. Lindgren, A. Doria, O. Schelen, Probabilistic routing in intermittently connected networks, SIGMOBILE Mobile Computing Communications Review 7 (3) (2003) 19–20.