Volume : 2 | Issue : 11 | Nov 2013 • ISSN No 2277 - 8160

Research Paper | Engineering

Improving the Quality of Service of Routing Protocols in Wireless Network

Mr. VinodhKumar. A	M.E(Asst Professor), AIHT, Chennai, Tamil Nadu, India
Ms.Bhargavi.P	B.Tech(Student),AIHT,Chennai,Tamil Nadu,India
Ms. Muthulakshmi. D	B.Tech(Student),AIHT,Chennai,Tamil Nadu,India

ABSTRACT

In adhoc networks, routes may be disconnected due to dynamic movement of nodes. So, route selection and topology combination is very difficult and challenging issue. Such networks are more vulnerable to both internal and external attacks due to presence of bad neighbor nodes. For point-to-point communication network on which a number of information sources are to be mulitcast to certain sets of destinations. In general it is not optimal to regard the information to be multicast as a "fluid" rather, by employing coding at the nodes, which we refer to as network coding, bandwidth can in general be saved. An improvement of the neighbor detection algorithm based on the differentiation of good and bad neighbors using signal to noise ratio (SNR) value is proposed. A network layer security solution SCAN exploits localized collaboration and information cross-validation to protect the network in a self-organized manner. In this paper, impact of bad neighbor nodes in adhoc routing is briefly discussed and proposed a method (GNDA) for identifying good neighbor nodes in the network using AODV routing protocol. The result of this paper is an appropriate solution against neighbor attacks.

KEYWORDS : MANETs, adhoc routing, AODV, SCAN, Network coding, SNR, Localized collaboration, Information cross-validation.

1. INTRODUCTION

In adhoc networks, routes may be disconnected due to dynamic movement of nodes. So, route selection and topology combination is very difficult and challenging issue. Such networks are more vulnerable to both internal and external attacks due to presence of bad neighbor nodes. For point-to-point communication network on which a number of information sources are to be mulitcast to certain sets of destinations. In general it is not optimal to regard the information to be multicast as a "fluid" rather, by employing coding at the nodes, which we refer to as network coding, bandwidth can in general be saved. An improvement of the neighbor detection algorithm based on the differentiation of good and bad neighbors using signal to noise ratio (SNR) value is proposed. A network layer security solution SCAN exploits localized collaboration and information cross-validation to protect the network in a self-organized manner. In this paper, impact of bad neighbor nodes in adhoc routing is briefly discussed and proposed a method (GNDA) for identifying good neighbor nodes in the network using AODV routing protocol. The result of this paper is an appropriate solution against neighbor attacks.

Index Terms-- MANETs, adhoc routing, AODV, SCAN, Network coding, SNR, Localized collaboration, Information cross-validation.

In this paper, performance of network increases rapidly by considering good nodes into the account. Categorizations of good and bad nodes depend upon signal strength, flow capacity of nodes. Moreover, how fast each node can receive the complete information. Proposed approach is analyzed by using AODV routing protocol. In existing computer networks, each node functions as a switch in the sense that it either relays information from an input link to an output link, or it replicates information received from an input link and sends it to a certain set of output links. From the information-theoretic point of view, there is no reason to restrict the function of a node to that of a switch. Rather, a node can function as an encoder in the sense that it receives information from all the input links, encodes, and sends information to all the output links. From this point of view, a switch is a special case of an encoder. In the sequel, we will refer to coding at a node in a network as network coding. We tackle an important security issue in adhoc networks, namely the protection of their network-layer operations from malicious attacks. We focus on securing the packet delivery functionality because it is the premise for the multihop connectivity between two faraway nodes. Without appropriate protection, the malicious nodes can readily function as routers and prevent the network from correctly delivering the packets. For example, the malicious nodes can announce incorrect routing updates which are then propagated in the network, or drop all the packets passing through them.

Implementation of routing protocols is developed by using Linux-5.3 and ns2.33[5]. In adhoc mode, we have used IEEE 802.11a for this approach.

2. OVERVIEW OF THE AODV

AODV belongs to the group of reactive routing protocols. These protocols initiate route discovery only when a route is needed and maintain active routes only while they are in use. Unused routes are deleted.

A. Route Discovery

When a new route is needed, the source node broadcasts a Route Request message (RREQ). Any node with a route to the destination responds by sending a Route Reply message (RREP) to the source node. If the node does not have a route to the requested destination, it rebroadcasts the RREQ. When the source node receives a RREP, the route is established and the source can start using it.

B. Local Connectivity

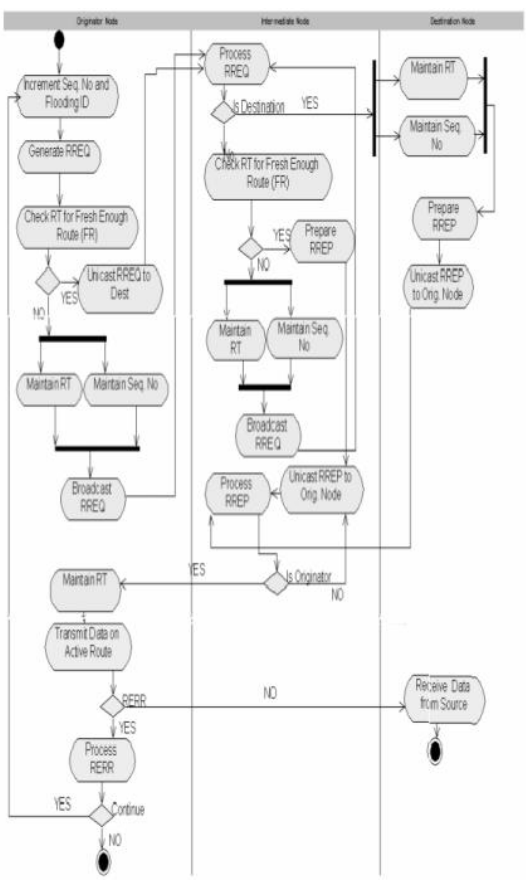
A node may offer connectivity information by broadcasting Hello messages periodically. When a Hello message is received, a route to the neighbor is added to the routing table if it does not already exist.

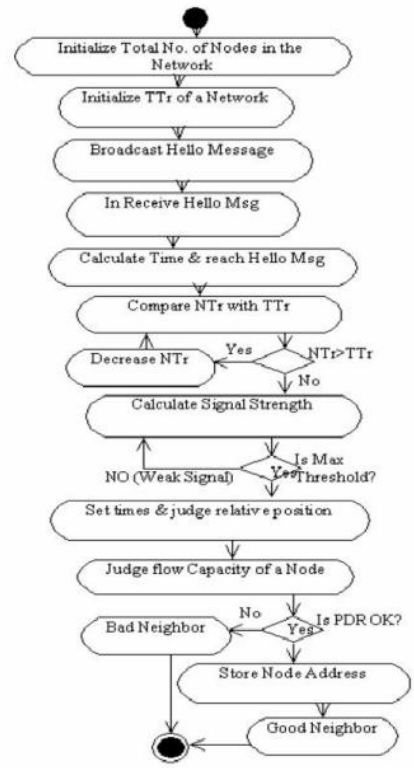
If the route exists, its lifetime is increased. When the topology of the ad hoc network changes and Hello messages are not received for a defined period of time, the route expires.

3. PROCESS FLOW OF GNDA

In this approach, initially all nodes maintain their own transmission range. It has been assumed the transmission range of the network is 250 meters. Now, transmission range (NTr) of each node present in the network with the total transmission of network (TTrN) of the node is compared. Determination of transmis-

sion power is required to send a message between node n and its neighbor n1. It can be measured by calculating the received power of hello message. When node n receives hello messages from a neighbor node n1, it can estimate the minimum power level needed to reach n1 by comparing the received power of hello message with maximum transmit power. This approach is enhanced by adding parameters in the neighbor table such as flow capacity, signal strength. Reaching time of hello messages between node and its neighbor is calculated. Address of node is stored into the neighbor table based on their transmission range. If (NTr > TTrN), then adjust energy of this node accordingly, otherwise calculate signal strength by using equation (1). If threshold value is maximum then evaluate position of node and also set timer for the same. Further work is preceded by calculating the flow capacity of a node as mentioned in equation (2). If flow capacity of a node is good then store address of a node otherwise remove address of the node from routing table. Suggested algorithm is an optimal solution for finding good nodes. Categorization of nodes is based on performance metrics such as transmission range and power of node, signal strength, capacity of node for high packet forwarding and relative position of node. Neighbor routing table maintains address of node for maintaining record of the entire nodes. These stored nodes are used for data transmission and forwarding. This approach minimizes energy consumption of node and increases its battery life. Thus any node can forward data to other node if they exist with in the range of 250 meters. And location or relative position of node can be verified by using routing table.





Definition1: Signal Strength of a node is computed by using well known formula which is as follows:

$$Transmitter_{signal\,strength} =$$

$$\begin{cases} S_H - \left\{\dfrac{S_H - S_{threshold} * T}{e}\right\} & if\ farther (T < e) \\ S_H & closer\ (T < e) \\ S_{thresh} & Otherwise \end{cases}$$

(1)Where SH is signal strength of hello message and T is the time period between two successive hello packets and e is the link connectivity between i and j.

Definition2: Assume a graph G (V, E) [13]. The capacity of directed edge is denoted as Cij source s and destination d. F is assumed as a flow in G where E belongs to edge (i, j).If for all (i, j) Є E; 0<= Fij <=

Cij; s.t.

(2)Let Fis and Fsj be the counter of amount of bytes that flowed on the link (i, j) upto time t in packets. Thus, If signal strength range is negligible then discard this node and delete entry of this node from the neighbor table. Otherwise calculate flow capacity of a node by considering equation (2). Based on flow capacity and packet delivery ratio, good neighbors are identified.

$$\sum_{j:(s,j)\in E} F_{sj} - \sum_{i:(i,s)\in E} F_{is}$$

4. SCAN DESIGN

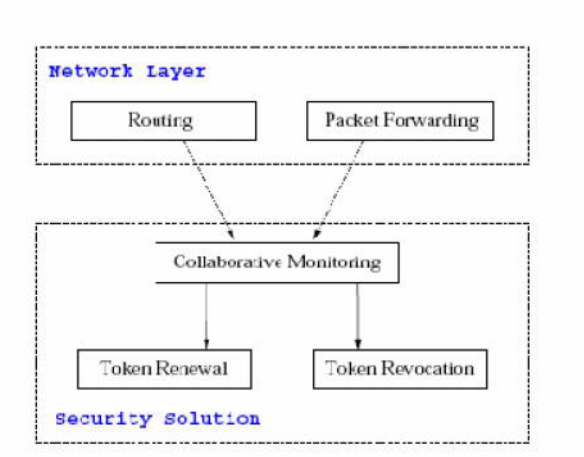
In this section we present the SCAN design in details. In order to protect the packet delivery functionality, each SCAN node overhears the wireless channel in the promiscuous mode, and monitors the routing

and packet forwarding behavior of its neighbors at all time. The monitoring results at different nodes in a local neighborhood are cross-validated. A malicious node is convicted when its neighbors have reached such a consensus, then it is deprived of the network membership and isolated in the network. In order to enforce the network access, each legitimate node carries a valid token which certified, unexpired, and not revoked, while any node without a valid token is denied of participation in the network operations. A legitimate node can always renew the token from its neighbors before its current token expires. However, when a malicious node is convicted, its neighbors collectively revoke its current token and inform all other nodes in the network. The above SCAN framework is illustrated in Figure 1, which has the following three components:

Collaborative Monitoring: all nodes within a local neighborhood collaboratively monitor each other.

Token Renewal: all legitimate nodes in a local neighborhood collaboratively renew the tokens for each other

Token Revocation: the neighbors of a malicious node, upon consensus, collaboratively revoke its current token. In this framework, the malicious nodes are detected and convicted via the collaborative monitoring mechanism, which collects and analyzes each node's behavior in the routing and packet forwarding activities.



The token revocation mechanism reacts to occasional attacks launched by the malicious nodes by revoking their tokens and alerting the network. This proactively prevents a convicted attacker from further disrupting the network operations, because without a valid token, it can not participate in the network any more. The token renewal mechanism ensures that legitimate nodes can continue to stay in the network by renewing their token from time to time. The above seemingly simple operations pose several research challenges. For example, how can we provide "anytime, anywhere" token renewal with low overhead? How can each node monitor the behavior of its neighbors? How accurate the monitoring results are, and how can we improve this accuracy? Given that the malicious nodes may roam in the network, what is the effective way to isolate them in the network?

5 .CONCLUSION

All information related with good neighbors are stored in routing table which improves performance of routing protocol in terms of good communication and stable route. Suggested approach demonstrate high quality in terms of good packet delivery and throughput which is almost above 90% where as performance of AODV lies between 80%-85%. Analytical results shows that it improves data throughput, improve overall performance of the network with in fixed and dynamic transmission range.

REFERENCES

[1] Umang Singh, Prof. B. V. R. Reddy , Prof M. N. | Hoda ,"GNDA: Detecting good neighbor nodes in adhoc routing protocol",2011 Second International | Conference on Fig. 1. The SCAN framework: components and interactions. Emerging Applications of Information Technology. | | [2] H. Yang, X. Meng, and S. Lu, Self Organized Network-Layer Security in Mobile Ad hoc Networks. International Conference on Mobile Computing and Networking, Atlanta, GA, USA, 2002, 11-20. | | [3] Srdjan Krco and Marina Dupcinov, "Improved | | Neighbor Detection Algorithm for AODV Routing Protocol", IEEE COMMUNICATIONS LETTERS, | VOL. 7, NO. 12, DECEMBER 2003. | | [4] P.Santi, "Topological Control in Wireless Adhoc and Sensor Networks", John Wiley & Sons | Ltd.,2005. | | [5] Rudolf Ahlswede, Ning Cai, Shuo-Yen Robert Li, and Raymond W.Yeung, "Network Information | Flow, IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 46, NO. 4, JULY 2000, 0018– 9448/00$10.00 © 2000 IEEE. | |