ISSN:2348-2079

Volume-5 Issue-2

International Journal of Intellectual Advancements and Research in Engineering Computations

Robust ad-hoc sensor routing (RASER) protocol for mobile wireless sensor networks

[1]Mr.C.Mani M.C.A., M.PHIL., M.E., Associate Professor,
[2]Ms. S. Gowsalya Final MCA,
Department of MCA, Nandha Engineering College (Autonomous), Erode-52.
Email-ID: cmanimca@gmail.com, Gowsalya9495@gmail.com

Abstract*— Sensor networks are an important tool for monitoring physical phenomena in the modern world. The nodes ability to communicate wirelessly removes the need for long wires and enables them to be distributed in an ad-hoc manner wherever and whenever required. One of the main challenges in these Mobile WSNs (MWSNs) is the routing protocol, which aims to transport the data generated by the sensors to the sink. A constantly changing topology means that a fixed path from a sensor to the sink cannot be guaranteed. The more demanding applications also require the consistent delivery of real-time data in highly mobile scenarios. Robust Ad-hoc Sensor Routing (RASeR) protocol is designed to be a reliable solution, even with the high frequency topology changes of a mobile network. It uses a simple hop-count gradient to allow sensor nodes to blindly forward data towards a single sink. A key issue with this type of routing is in keeping the gradient metric up to date, for this reason RASeR uses a design that combines a Global Time Division Multiple Access (GTDMA) medium access control (MAC) scheme with the routing protocol. In proposed work, the communication in Mobile Ad-Hoc Network (MANET) is based on mutual trust between the participating nodes. Due to features of open medium, dynamic changing topology, lack of centralized monitoring and management, MANETs are vulnerable to various security attacks. Hence, finding a secure and trustworthy end-to-end path in MANET is a real challenge. Our analysis shows significant improvement in packet delivery ratio of AODV in the presence of attacks, with marginal rise in control traffic Overhead.

INTRODUCTION

Sensor networks are an important tool for monitoring physi-cal phenomena in the modern world, since they often negate the need for human presence. The nodes' ability to communicate wire-lessly removes the need for long wires and enables them to be distributed in an ad-hoc manner wherever and wheneve r required, which could include harsh and hostile terrains. For this rea-son, along with the availability of low cost nodes, Wireless Sensor Networks (WSNs) are already commonplace in industry and are be-coming more and prevalent in the consumer market. Furthermore, the introduction of mobility to WSNs is an open research issue and can realise the potential for many more emerging applica-tions and will be a key enabling technology in the future of ubiq-uitous sensing. There are an increasing number of applications for which a MWSN may be utilised, such as wildlife monitoring, environ-ment mapping and traffic monitoring in smart cities. There are also applications in emergency scenarios such as the mon-itoring of vital signs in temporary hospitals and the use of un-manned aerialvehicles (UAVs) in the aiding of search and rescue (SAR) .

SYSTEM METHODOLOGY

TRUST MANAGEMENT SCHEME

In on-demand routing protocols, it is argued that if a node has monitored a route reply (RREP) packet then it must have monitored its corresponding route request (RREQ) packet. The cross-correlation between RREP and RREQ monitored packets with respect to a source and destination pair reveals the behavior of nodes in the MANET.

About that node. Similar cross-correlation can also be established with DATA packets and RREP control packets. Such cross-correlation from the monitored traffic is instrumental in detection of malicious nodes by the monitor in MANET. Since bad guys must be punished heavily, hence additive increment for positive experiences and multiplicative decrement for negative experiences are employed in computation of reputation rating.

The pairing between different types of monitored unicast packets, such as ACK and DATA, DATA and RREP, can easily be made by looking their source and destination addresses in IP headers. However, pairing between monitored

packets that involve broadcast messages, such as RREP and RREQ, RERR and RREQ. In broadcast messages, since the destination address is always a broadcast address, to keep track of such messages source address in IP header is utilized as previous node address that forwarded the broadcast message.

TRUST BASED ROUTING PROTOCOL

The proposed trust based routing protocol in the MANET architecture, with the help of an example, as shown in Fig. 1. The MANET architecture has two categories of nodes i.e. Trusted Mobile Node (TdMN) and Truster Mobile Node (TrMN). TdMNs are trusted ones and every TrMN is associated with one of the TdMNs within its communication range pronounced as Associated Trusted Mobile Node (ATMn).

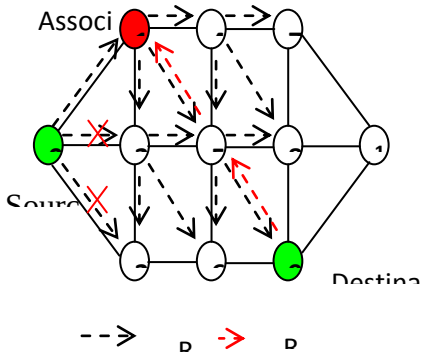

Fig.(a). Trust based routing: Route Request (RREQ) and Route Reply (RREP)

The choice of a TdMN is solely at the discretion of the TrMN. All the Mobile Nodes use this routing protocol. The proposed routing protocol is an adapted AODV routing protocol. The path between source and destination always includes the ATMn of the source. Assumption 1: The wireless communication links between the Mobile Nodes are symmetric and bidirectional.

Assumption 2: Each wireless interface operates in promiscuous mode.

Assumption 3: Destination Mobile Node and TdMNs are not malicious.

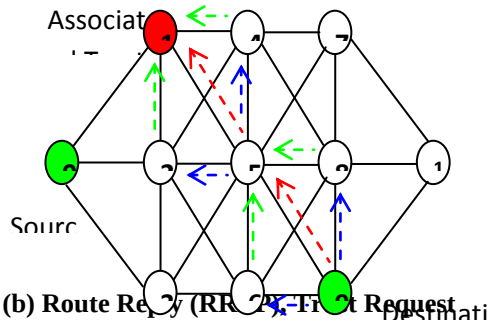

Fig (b) Route Reply (RREP), Trust Request (TREQ) and Trust Reply (TREP)

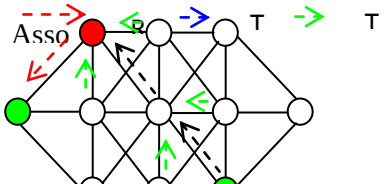

Fig (c) Route Reply (RREP) and Trust Evaluate (TEVAL)

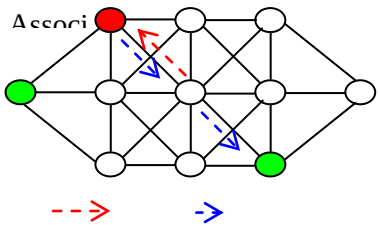

Fig (d) Trust Evaluate Acknowledgment (TEVAL ACK) and Route Reply (RREP)

The protocol involves the following processes:

a) Route Discovery,

b) Route Maintenance,

c) Dealing with malicious nodes and

d) Admission of new nodes.

A) Route Discovery

The route discovery process is described as follows.

1) Source Mobile Node broadcasts route request (RREQ) message in order to find a route to destination Mobile Node (in Fig. 1(a)).2) Among neighbors of the source Mobile Node, only the ATMn of the source forwards the RREQ message if either it does not have a fresh route to the destination or it has a fresh route to the destination but with path trustworthiness below a threshold value (PATH THRESHOLD). Path trustworthiness at the ATMn is the trustworthiness of the path from the ATMn of the source to the destination. All other neighbors drop the RREQ message (in Fig. 1(a)).

3) All neighbors of the ATMn further forward the RREQ message to their neighbors, and so on, until either the destination or an intermediate Mobile Node

with a fresh route to the destination and path trustworthiness above PATH THRESHOLD is reached (in Fig. 1(a)). Path trustworthiness at an intermediate Mobile Node is the trustworthiness of the path from the intermediate node to the destination.

4) The destination or an intermediate Mobile Node with a fresh route to the destination and path trustworthiness above PATH THRESHOLD replies by a route reply (RREP) message to the ATMn of the source (in Fig. 1(a)).

5) During the process of sending/forwarding the RREP message, everyMobile Node in the reverse path broadcasts trust request (TREQ) message, shouting for trust value of the nexthop Mobile Node in the upstream from its neighbors (in Fig. 1(b)). The broadcast is only to one-hop Mobile Nodes.

6) Upon receipt of TREQ message, the neighbors broadcast trust reply (TREP) message with trust value of the upstream Mobile Node in their respective node trust table (in Fig. 1(b)). The broadcast is only to one-hop Mobile Nodes.

7) Upon receipt of TREP messages, the neighbors including upstream Mobile Node accumulate TREPs in their trust reply table, as in (2).

8) The ATMn of the source Mobile Node, upon receipt of the RREP message, buffers the RREP till trustworthiness of the discovered path is evaluated.

9) In order to evaluate the trustworthiness of the discovered path, the ATMn of the source Mobile Node unicasts trust evaluate (TEVAL) message to the destination with a FLAG set (in Fig. 1(c)). The FLAG is set to ensure that its acknowledgment is only from the destination node.

10) Upon receipt of TEVAL, the destination Mobile Node replies with trust evaluate acknowledgment (TEVAL ACK) message back to the ATMn of the source Mobile Node with path trust value as ZERO (in Fig. 1(d)).

11) During the process of receiving/forwarding the TEVAL ACK (in Fig. 1(d)), the intermediate Mobile Nodes compute node trustworthiness from the accumulated TREPs in their respective trust reply table by using (3). If the received path trust value is less than the PATH THRESHOLD then the TEVAL ACK is dropped else the computed node trustworthiness is added with the received path trust value in TEVAL ACK message, as in (4), to compute trustworthiness of the path from the intermediate node to the destination. The intermediate Mobile Nodes update trust value with respect to the destination in their respective path trust table and path trust value in TEVAL ACK message before forwarding the TEVAL ACK message to its upstream Mobile Node.

12) The ATMn of the source Mobile Node forwards the buffered RREP to the source only if the evaluated trustworthiness of the discovered path is above PATH THRESHOLD (in Fig. 1(d)).

13) The source Mobile Node selects the route only if it has received the RREP message from its ATMn.

B) Route Maintenance

When a link break occurs in an active route, the node upstream of that break chooses to repair the link locally if it is closer to the destination. To repair the link break, the repairing node broadcasts a RREQ message for the destination.

Since such RREQ message is in response to local link repair, it does not warrant being through ATMn of the repairing node. If the repairing node receives a RREP then the route is locally repaired, otherwise it transmits a route error (RERR) message to its precursors.

When the source node receives the RERR message the source node rediscovers the route. In the proposed trust based routing protocol, trustworthiness of the locally repaired path is not evaluated. This is to avoid packet drops at the Mobile Node that initiates local repair.

C) Dealing with Malicious Nodes

Since all ongoing communication are tapped by Mobile Nodes, behavior of neighboring Mobile Nodes gets reflected into their node trust table by using (1). A Mobile Node broadcasts an alarm message (TREP with alarm) if it detects a node with trust value bellow a threshold (NODE TRUST THRESHOLD) as malicious. Upon receipt of such alarm messages, if a neighboring node has route in its routing table with nexthop as the detected malicious node address then it deletes the route from its routing table and handles it as in route maintenance.

Mobile Nodes use alarm node trust table and ALARM THRESHOLD to deal with malicious Mobile Nodes. If the number of alarm messages received for a Mobile Node is more than ALARM THRESHOLD then the route is deleted and RERR message is generated.

D) Admission of New Nodes

New Mobile Nodes, joining the network, wait for DELETE PERIOD [16] before transmitting any route discovery messages. During the DELETE PERIOD, new Mobile Nodes receiving control packets create route entries but do not forward any control packets. Further, during the same, the new Mobile Nodes build their node trust table from their monitored traffic, as in (1).

Based on the trust values in the node trust table, a new Mobile Node gets associated with one of the TdMNs with the highest node trust value.

EXISTING SYSTEM

RASeR uses the blind forwarding technique to forward data along a gradient towards the sink, so the decision to forward data is made at the receiving node on a hop by hop basis. In other words, when a node transmits, its broadcast is overheard by all of its neighbors. Each neighbor can then compare the hop count contained in the received packet with its own. Subsequently, if the node's hop count is less than the received hop count, then the packet should be forwarded. If the node's hop count is greater than the received hop count, then the packet should be dropped.

Alternatively, if the node's hop count and the received hop-count are equal the packets status should be taken into account. The priorities are used to control the number of routes a packet may take, in this way the redundancy can be kept to a minimum, whilst still increasing the protocol's reliability. Each packet has a priority bit, which designates its status as either priority status or diversity status. The status of a packet is indicated by the state of its priority bit, which differentiates between priority packets and diversity packets. When a node receives a packet it stores it in a queue, so before a nodes time slot it must decide which packet to transmit packets with priority status are given precedence over those with diversity status.

DRAWBACKS

- It is not suitable for highly scalable and dynamic networks
- It increases overhead and end to end delay

PROPOSED SYSTEM

The proposed system deals with trust based routing protocol in the MANET architecture. The MANET architecture has two categories of nodes i.e. Trusted Mobile Node (TdMN) and Truster Mobile Node (TrMN). TdMNs are trusted ones and every TrMN is associated with one of the TdMNs within its communication range pronounced as Associated Trusted Mobile Node (ATMn).

The choice of a TdMN is solely at the discretion of the TrMN. All the Mobile Nodes use this routing protocol. The proposed routing protocol is an adapted AODV routing protocol. The path between source and destination always includes the ATMn of the source.

Assumption 1: The wireless communication links between the Mobile Nodes are symmetric and bidirectional.

Assumption 2: Each wireless interface operates in promiscuous mode.

Assumption 3: Destination Mobile Node and TdMNs are not malicious.

ADVANTAGES

- The proposed system shows that EAODV1, EAODV2 and AAODV are very simple techniques and require substantially less knowledge of the network.
- Depending on the nature of movement of the nodes the new system can select EAODV1, EAODV2 or AAODV.
- In addition, the new system shows that EAODV1 is best suited for networks where movement of the nodes is moderate, EAODV2 is best suited for networks where the movement of the nodes is fast and AAODV is best suited for networks where the movement of the nodes is at varying speeds at different point of time.
- It is suitable for highly scalable and dynamic networks as it has drastically reduced the amount of overhead, improved PDR and reduced end to end delay in the popular reactive routing protocol AODV in different mobility scenarios.

Hop count determination

The hop count is a simple metric, which indicates a node's dis-tance in hops from the sink. Local topology information is shared to maintain

this hop count at each node. The hop-counts are then used to ensure data is always forwarded towards the sink.

Even though the nodes will often require location awareness for reporting positions to the sink, it is still preferable to use a hop count metric for routing. This is because the location information is not considerate of the topology, which can cause issues such as the dead-end problem.

Using the GTDMA MAC, each node has the opportunity to trans-mit once in a cycle. In every slot nodes are required to transmit a data packet, or a beacon packet if the node has no data to forward. A beacon packet is simply the first two fields of the data packet, namely the node ID and hop count. In this way, each node will have the chance to overhear the transmission of every node that's in range, before its own timeslot comes around. In other words a node determines its position in the network us-ing only the topology information, which is the hop count in this case, that is locally available to it from its one-hop neighbours.

Forwarding data

RASeR uses the blind forwarding technique to forward data along a gradient towards the sink, so the decision to forward data is made at the receiving node on a hop by hop basis. In other words, when a node transmits, its broadcast is overheard by all of its neighbours. Each neighbour can then compare the hop count contained in the received packet with its own. Subsequently, if the node's hop count is less than the received hop count, then the packet should be forwarded. If the node's hop count is greater than the received hop count, then the packet should be dropped. Alter-natively, if the node's hop count and the received hop-count are equal the packets *status* should be taken into account.

CONCLUSION

In mobile ad hoc networks (MANETs), each node works not only for itself but also for other nodes. Under such environment, some nodes may misbehave for individual interests. So reputation and trust are instrumental to deal with such misbehaving nodes. Further, in an application perspective MANETs, they are equally prone to security threats as that are in wireline networks. In this thesis, the proposed solution has not only made the feasibility for placement of firewalls to thwart security threats that are common to wireline networks, but also exploited dynamic and cooperative features of MANETs to deal with misbehaving nodes in discovering trustworthy path. Future work includes cross-correlation of monitored traffic under mobility scenarios. The simulation application works well for given tasks in network environment. Any system with .Net framework installed can execute the application. The application reduces the difficulties in the existing system. It is developed in a user-friendly manner. The application is very fast and any transaction can be viewed or retaken at any level. The project provides a best assistance in trust worthy path discovery in MANETs. The following options can be added in future. In future, cross-correlation of monitored traffic under mobility scenarios can be studied. The developed application can be designed as a web site so that it can be accessed across the platforms.

REFERENCES

[1] X. Li, et al., Performance evaluation of vehicle-based mobile sensor networks for traffic monitoring, IEEE Trans.Veh.Technol.58(4) (2009) 1647–1653.

[2] D. Ni. Determining traffic-flow characteristics by definition for application in ITS. IEEE Trans on ITS, 2007.

[3] Y. Cho. Estimating velocity fields on a freeway from lower solution videos. IEEE Trans on ITS, v 7, n 4, pp. 463-469,200.

[4] K. Lorincz, et al., Sensor networks for emergency response : challenges and opportunities, IEEE PervasiveComput.3(4) (2004) 16–23.

[5] S. Bohacek, Performance improvements provided by route diversity in multihop wireless networks, IEEE Trans.MobileComput.7(3) (Mar. 2008)372–384.

[6] P. Sambasivam, A. Murthy, and E. M. Belding-Royer, "Dynamically adaptive multipath routing based on AODV," in MedHocNet, 2004.

[7] M. K. Marina and S. R. Das, "Ad hoc on-demand multipath distance vector routing," tech. rep., SUNY - Stony Brook, 2003.

[8] A. Nasipuri and S. R. Das, "On-demand multipath routing for mobile ad hoc networks," in Proceedings of IEEE International Confernce on Computer Communications and Networks ICCCN, pp. 64–70, 1999.

[9] S.-J. Lee and M. Gerla, "AODV-BR: backup routing in ad hoc networks," in IEEE WCNC, pp. 1311–1316, 2000.[10] L. Zhang, Z. Zhao, Y. Shu, L. Wang, and O. W. Yang, "Load balancing of multipath source routing in ad hoc networks," in Proceedings of IEEE ICC'02, 2002.

[11] J. Al-Karaki, A. Kamal, Routing techniques in wireless sensor networks : A Survey, IEEE WirelessCommun.11(6) (2004) 6–28.

[12] W. Heinzelman, A. Chandrakasan and H. Balakrishnan, "Energy-Efficient Communication Protocol for Wireless Microsensor Networks," Proceedings of the 33rd Hawaii International Conference on System Sciences (HICSS '00), January 2000.

[13] F. Ye, A. Chen, S. Liu, L. Zhang, "A scalable solution to minimum cost forwarding in large sensor networks", Proceedings of the tenth International Conference on Computer Communications and Networks (ICCCN), pp. 304-309, 2001.