International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue-17
December 2017

Security Intensification for Mobile Ad Hoc Networks with Reliable Management Using Uncertain Reasoning

Gorati aruna & Dr.Srihari Rao
PG Scholar, Director, Professor, Department Electronics & Communication Engineering(WMC),
Bharat Institute of Engineering and Technology, Mangalpally, Ibrahimpatanam, Hyderabad, Telangana

Abstract:

Ad hoc networks as well alleged basement beneath networks are circuitous broadcast systems abide of wireless links amid the nodes and anniversary bulge as well works as a router to assiduously the abstracts on account of added nodes. The nodes are charge less to accompany or larboard the arrangement after any restriction. Thus the networks accept no abiding infrastructure. In ad hoc networks the nodes can be anchored or mobile. Therefore one can say that ad hoc networks basically accept two forms, one is changeless ad hoc networks(SANET) and the added one is alleged adaptable ad hoc networks(MANET). With contempo advances in wireless technologies and adaptable devices, Adaptable ad hoc networks accept become accepted as a key advice technology in aggressive appropriate environments. There are mainly two problems in aegis techniques, one is depends on the key administration and added one is to depends on some average nodes. We adduce a unified assurance administration arrangement that enhances the aegis in MANETs. In our scheme, The abode of an adjoining bulge is acclimated as allurement destination abode to allurement awful nodes to forward a acknowledgement RREP message, and awful nodes are detected application a about-face archetype technique.

Our ultimate ambition in this activity is 1)to ascertain the awful bulge if it drops the packets,2)to accommodate the top end apprehension adjustment for gray-hole collaborative advance in MANET.3)To account assurance amount and accommodate the aegis based on the acquaintance assessment trust ,4)Defending adjoin fake reply

Key word: MANET, Security, Trust management, AODV

*1)*Introduction:

Wireless networks can be basically either infrastructure based networks or infrastructure less networks. The infrastructure based networks uses fixed base stations, which are responsible for coordinating communication between the mobile hosts (nodes). The ad hoc networks falls under the class of infrastructure less networks, where the mobile nodes communicate with each other without any fixed infrastructure between them. An ad hoc network is a collection of nodes that do not rely on a predefined infrastructure to keep the network connected. So the functioning of Ad-hoc networks is dependent on the trust and co-operation between nodes. Nodes help each other in conveying information about the topology of the network and share the responsibility of managing the network. Hence in addition to acting as hosts, each mobile node does the function of routing and relaying messages for other mobile node

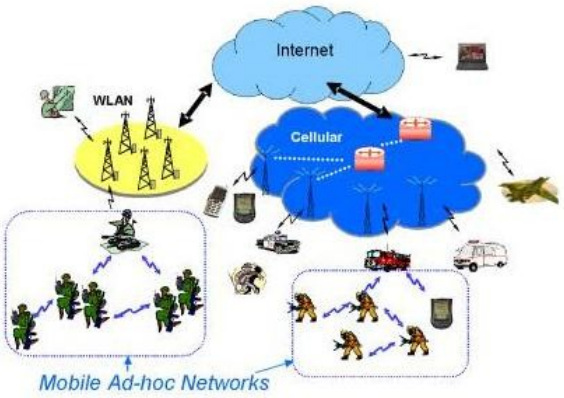

Fig. 1 Mobile ad-hoc network

2)Related work

Peer-to-peer networks are networks in which peers cooperate to perform a critical function in a decentralized manner. All peers are both consumers and providers of resources and can access each other directly without intermediary peers. Compared with a centralized system, a peer-to-peer (P2P) system provides an easy way to aggregate large amounts of resources residing on the edge of Internet or in ad-hoc networks with a low cost of system maintenance. P2P systems have attracted increasing attention from researchers recently, but they also bring up some problems. Since peers are heterogeneous, some peers might be benevolent in providing services. Some might be buggy or malicious and cannot provide services with the quality that they advertise. Since there is no centralized node to serve as an authority to monitor and punish the peers that behave badly, malicious peers have an incentive to provide poor quality services for their benefit because they can get away. Some traditional security techniques, such as service providers requiring access authorization, or consumers requiring server authentication, are used as protection from known malicious peers. However, they cannot prevent from peers providing variable-quality service, or peers that are unknown. Mechanisms for trust and reputation can be used to help peers distinguish good from bad partners. This paper describes a trust and reputation mechanism that allows peers to discover partners who meet their individual requirements through individual experience and sharing experiences with other peers with similar preferences.

In our model a peer builds two kinds of trust in another peer, say peer A and peer B respectively. The first one is the trust that peer A has in peer B's capability in providing services. The other is the trust that peer A has in peer B's reliability in providing recommendations about other peers. Here the reliability includes two aspects:

Truthfulness – whether peers B is truthful in telling its information

Similarity – whether peers B is similar to peer A in preferences and ways of judging issues.

In the upcoming generation of wireless communication technology, there will be a need for the rapid deployment of independent mobile users. Substantial examples include establishing survivable, dynamic, efficient communication for emergency/rescue operations, military, and disaster relief effort networks. Such technology scenarios cannot rely on centralized and organized infrastructure, but can be conceived as applications of MANET. A Mobile Ad Hoc Networks is an autonomous collection of mobile users that communicate over relatively bandwidth constrained wireless ties. Since the nodes are movable, the network topology may change rapidly and unpredictably over time.

Technology is decentralized, where all network activity including discovering the topology and delivering messages must be executed by the nodes itself, i.e., the routing functionality will be incorporated into mobile node. In paper, an approach has been proposed to combat black-hole attack in AODV routing protocol. In this approach any node uses number rules to inference about honesty of reply's sender. Activities of a node in a very network show its honesty. To participate in information transfer method, a node should demonstrate its honesty. Early of simulation, all nodes area unit able to transfer data; so they need enough time to indicate its truth (Though each node are often a bearing less one). If a node is that the 1st receiver of a RREP packet, it forwards packets to supply and initiates judgment method on concerning replier. The judgment method is base on opinion of network nodes concerning replier. The activities of node information are logged by its neighbors table given in fig.3. These neighbors area unit requested to send their opinion a couple of node. Once a node collects all opinions of neighbors, it decides if the replier may be a malicious node. The choice is base on range rules. The subsequent rules employed in this paper to gauge concerning honesty of a node in network. This judgment is base on nodes are activity in network

3) Existing system & disadvantages:

There are two complementary classes of approaches that can safeguard tactical MANETs: prevention-based and detection based approaches. One issue of these prevention-based approaches is that a centralized key management infrastructure is needed, which may not be realistic in distributed networks such as MANETs. In addition, a centralized infrastructure will be the main target of rivals in battlefields. If the infrastructure is destroyed, then the whole network may be paralyzed. Serving as the second wall of protection, detection-based approaches can effectively help identify malicious activities. Although some excellent work has been done on detection based approaches based on trust in MANETs, observation in most approaches is only used to assess the reliability of nodes, which are not in the range of the observer node. Therefore, inaccurate trust values may be derived.

4)Proposed system & advantages:

We proposed the system with two observations one is direct and other one is indirect, in direct method each node can observe the behavior of other immediate nodes, and indirect model each node observes the information about multi-hop node by the immediate trustworthy node. We will use the history of the each immediate nodes behavior for direct observation. And reputation scheme for indirect observation.

By using the proposed trust management scheme we can get the accurate value and we can avoid the misbehavior nodes from the route.

In our base model, the researchers have used the direct observation by overhearing the information. This method will be best in some of the scenarios but this won't be good in all other scenarios

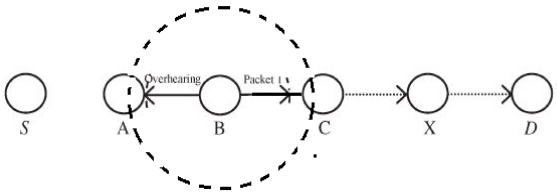

Fig.2 overhearing technique

The misbehavior node may capable of change the coverage area. In this situation the misbehavior may reduce the coverage it will show like forwarding the data to next node, but indeed the data won't be receive in next node.

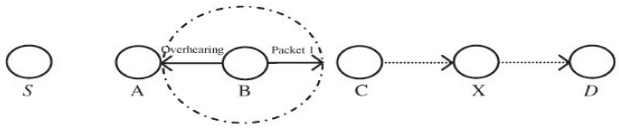

Fig.3. Overhearing method security problem

To avoid this problem we will introduce the technique for direct observation with end to end acknowledgement method with secret sign sharing.

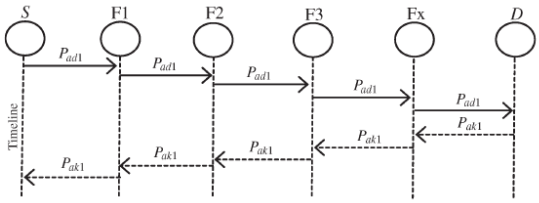

Fig.4 ACK based security implementation

In our enhancement work, we have addressed the problem of Energy based routing attack by using our base trust management work. Initially all nodes collects the data about neighbor nodes. The network monitors having the detailed information of neighbor nodes such as routing table. It provides the connection information to Route manager. The mobile devices periodically share their residual energy into all the nodes which are participating in the network. Based on this energy nodes will select the route in reliable. When source node sends RREQ, nodes will check the energy of all its one hop neighbor nodes. Then the node select the next node which one has high energy cost. All the nodes do the same process. Finally Destination node receive the RREQ and also it know the energy cost of both hop-by-hop also end-to-end communication. After validate these factors destination will send RREP through the high energy path. Each node need generate the Hello message in periodic interval. Own Energy level must be added into Hello message. Each node can able to receive the hello Message from neighbor node. Node has to extract the energy information from Hello message. Energy information should be stored into database for future use. Before storing Energy information, it has to be compared with old energy from database of same node. If old energy is more than new energy then the node will be considered as good node Or else the node will be malicious.

5) Algorithm:

Our ultimate aim in this project is to avoid malicious node in the route while communication. We are assuming that each node has the capability to detect nearest malicious node why because there are the number of implementation already have been done for detection methods, even though we are considered the simple algorithm which will detect the malicious in the route named as M-detection.

M-detection algorithm:

1) Define the control pkts
   a. RREQ
   b. RREP
   c. RERR
   d. Hello
2) Receive pkts
   a. If pkt is Hello
      i. Set as disturbance message is received
      ii. Start the message count
         1. If the message count is exceeds the threshold(variable)
            a. Check the Meli table
               i. If node not found
                  1. Add the node in table
               ii. Else
                  1. Ignore the message

Malicious prevention method:

1) If node has the data
   a. Check route cache
      i. If route is available
         1. Forward the data
      ii. If route is not found
         1. Initiate the route discovery
            a. Check the Meli cache
               i. If Meli found
                  1. Update the Meli info in RREQ
      iii. Send the broadcast the RREQ
2) If RREQ received
   a. Check the RREQ
      i. If Meli_list != Null
         1. Update Meli-table
   b. Check the Meli Table
      i. If forwarder ∈ table
         1. Ignore the message
      ii. If forwarder ∉Meli table
         1. For i∈ Meli table
            a. Updates "*i*" in RREQ
         2. If current node == destination of the pkt
            a. RREQ ⇒RREP
               i. Update the reverse route info
            b. Send to source
         3. If current node ≠destination
            a. Broadcast the RREQ as forwarder
3) Meli-maintenance routine
   a. If expire time<Current time
      i. Delete the Meli ID
4) If RREP is received
   a. Check the RREP
      i. If Meli_list != Null
         1. Update Meli-table
   b. Check the Meli Table
      i. If forwarder ∈ Meli table
         1. Ignore the message
      ii. If forwarder ∉Meli table
         1. If current node == destination of the pkt
            a. Update the reverse route info
            b. Send data pkt to destination
         2. If current node ≠destination
            a. For i∈ Meli table
               i. Updates "*i*" in RREP
            b. Forward RREP

Malicious node detection

1) If RREP received in source
   a. Check RREP Meli list

i. If list == Null **(***we planed to improve this in future with behavior checking)**
   1. Set the path as un trusted path
   2. Generate the OREQ
      a. Broadcast OREQ

2) If OREQ received
   a. set val = 0
   b. For "*i*" ϵ OREQ list
      i. If "*i*" ϵMeli table
         1. Generate the OREP
         2. Forward to source of OREQ
         3. Set Val = 1
         4. break
   c. if val ==0
      i. broadcast OREQ
3) if OREP received
   a. update the Meli information in Meli table

In this module, we have assumed that if reply contains empty malicious list then the route may contain malicious nodes, then the source node will get the doubt in the route. So the source will ask the opinion to other neighbor regarding malicious details. In future we will implement the history maintenance to check the behavior of the node so further we can improve the reliability in security on route.

Enhanced Energy based attacker avoidance algorithm

1) Set initial energy level for each node
2) Initialize Hello timer
3) If Hello timer triggered
   a. Generate the hello message
      i. Attach current energy
   b. Broadcast the pkt
4) If node has data
   a. If route is found
      i. Send data to next node
   b. Else
      i. Generate the req
         1. Attach energy level with pkt
      ii. Broadcast req
5) If node received packet
   a. If packet is hello packet
      i. Checks database
         1. If old energy is less than current energy
            a. Set as misbehavior node
   b. If packet is Req
      i. If received node is destination
         1. Check in routing table
            a. If old min energy is less than new
               i. Accept and send reply
            b. If old min energy is equal to new
               i. Checks the energy cost
                  1. If old cost is more than new
                     a. Accept and send reply
         2. ignore the packet
      ii. if node is intermediate node
         1. if pkt is duplicate or prev node is malicious
            a. ignore pkt
         2. Else
            a. Check in routing table
               i. Add the energy cost
               ii. If pkt min energy is more than own
                  1. Add own energy as min energy
               iii. Forward the pkt
   c. If pkt is Reply
      i. If prev node is malicious
         1. Ignore the packet
      ii. Else
         1. If node is not destination
            a. Forward the pkt

Result analysis:

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue-17
December 2017

We have tested our proposed system with the help of popular simulator (NS2). The fig.5 and 6 shows the animation result. And fig. 7-9 shows the graph result.

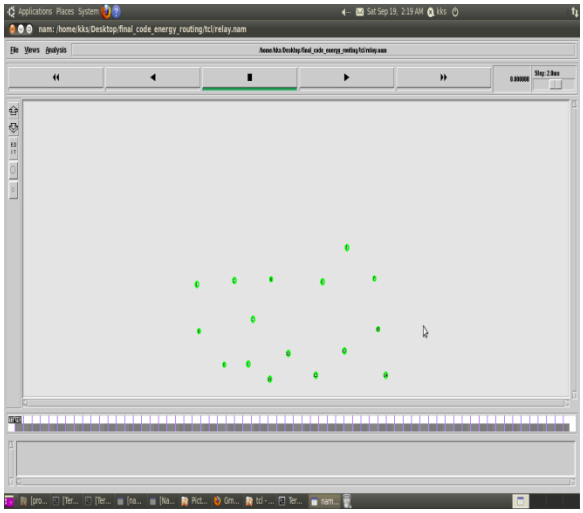

Fig.5 Network setup

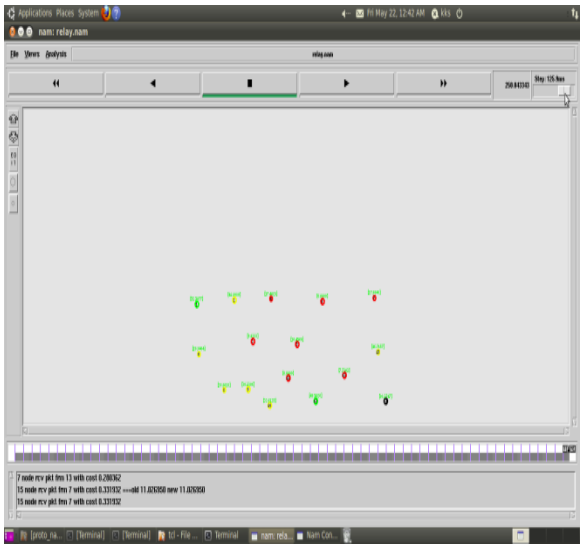

Fig.6 Node failure due to attack

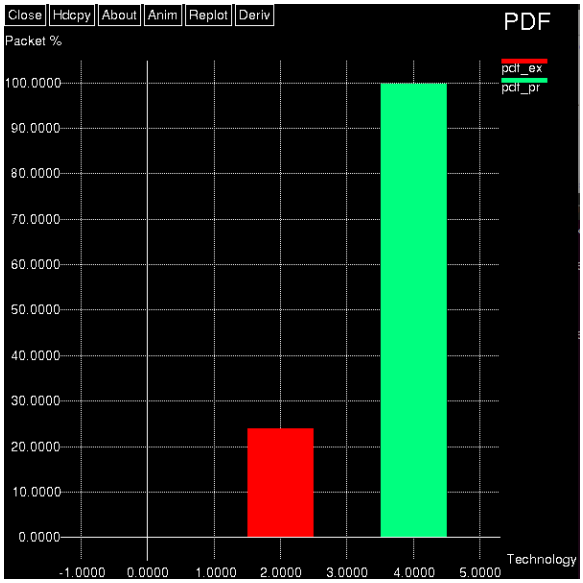

Fig.7 Packet delivery comparison (Enhanced system provides more packet delivery {green} than existing work)

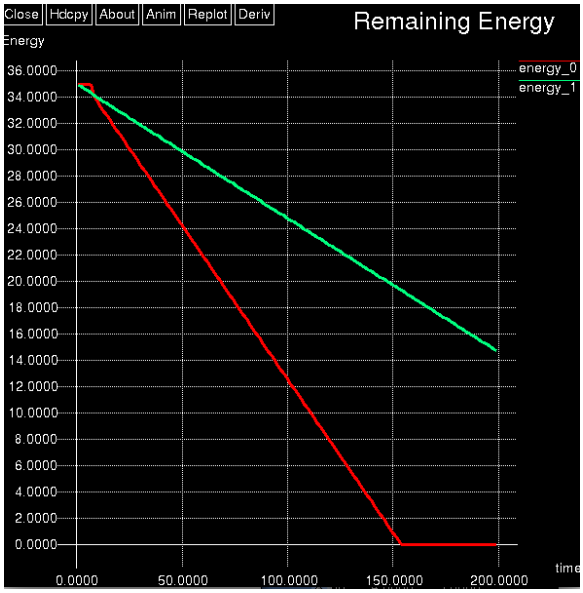

Fig.8 Energy comparison (our method provides high energy saving {green})

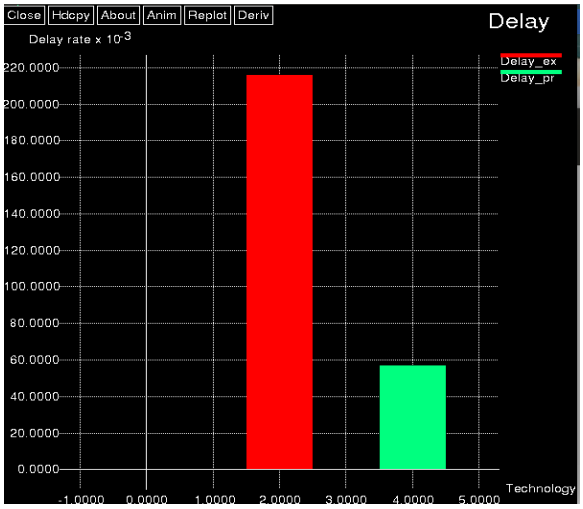

Fig.9 delay comparison (our method provides less delay {green})

Conclusion:

We have achieved our ultimate goal, which is to provide the security without relying on key management in MANET. We proposed a unified trust management scheme that enhances the security in MANETs. In this proposed trust management scheme, the trust model had two components: trust from direct observation and trust from indirect observation. We have test our enhanced energy based trust management system, which detects and eliminates the malicious node from the route. In our proposed solution we have considered the security based on the direct and indirect trust mechanism, in our future work to improve the security mechanism we will use position based trust management system.

Reference:

[1] "Trust and Reputation Model in Peer-to-Peer Networks", Yao Wang, Julita Vassileva

[2] "Design of Novel Agitation AODV routing protocol for defense against Black hole Attack", T.Bhavana, M.Tech (DECS), Sri Indu College of Engineering & Tech

[3] S. Corson and J. Macker, "Mobile ad hoc networking (MANET): routing protocol performance issues and evaluation considerations," IET RFC 2501, Jan. 1999.

[4] F. R. Yu, Cognitive Radio Mobile Ad Hoc Networks. New York: Springer, 2011.

[5] J. Loo, J. Lloret, and J. H. Ortiz, Mobile Ad Hoc Networks: Current Status and Future Trends. CRC Press, 2011.

[6] Q. Guan, F. R. Yu, S. Jiang, and V. Leung, "Joint topology control and authentication design in mobile ad hoc networks with cooperative communications," IEEE Trans. Veh. Tech., vol. 61, pp. 2674 – 2685, July 2012.

[7] F. R. Yu, H. Tang, S. Bu, and D. Zheng, "Security and quality of service (QoS) co-design in cooperative mobile ad hoc networks," EURASIP J.

[8] Wireless Commun. Networking, vol. 2013, pp. 188–190, July 2013.

[9] Y. Wang, F. R. Yu, H. Tang, and M. Huang, "A mean field game theoretic approach for security enhancements in mobile ad hoc networks," IEEE Trans. Wireless Commun., vol. 13, pp. 1616–1627, March 2014.

[10] J. Chapin and V. W. Chan, "The next 10 years of DoD wireless networking research," in Proc. IEEE Milcom'11, (Baltimore, MD, USA), Nov. 2011.