International Journal of Innovative Technologies
WWW.IJITECH.ORG
ISSN 2321-8665
Vol.04,Issue.01,
January-2016,
Pages:0058-0063

Improved Energy Based Security System for Mobile Ad-Hoc Networks with Belief Management System

K.KARTHEEKA[1], V.HARINI[2], S.SRINIVAS[3]

[1]PG Scholar, Dept of ECE, Vardhaman College of Engineering, Hyderabad, JNTUH, TS, India, Email: karthi.be21@gmail.com.
[2]Asst Prof, Dept of ECE, Vardhaman College of Engineering, Hyderabad, JNTUH, TS, India, Email: v.harini@vardhaman.org.
[3]Assoc Prof, Dept of ECE, Vardhaman College of Engineering, Hyderabad, JNTUH, TS, India, Email:s.srinivas@vardhaman.org.

Abstract: Our final goal is to realize the protection while not looking forward to key management in MANET with new trusting mechanism known as Trustworthy Energy management system. With recent advances in wireless technologies and mobile devices, Mobile Ad hoc Networks became widespread as a key communication technology in military plan of action environments. There square measure in the main 2 issues in security techniques, one is depends on the key management and another one is to depends on some intermediate nodes. We tend to propose a unified trust management theme that enhances the protection in MANETs. Within the proposed trust management theme, the trust model has 2 components: trust from direct observation and trust from indirect observation. And that we enhance our base work with energy trust management system. We'll use the quality AODV protocol to style SEMT protocol.

Keywords: MANET, Security, Trust Management, AODV Protocol.

I. INTRODUCTION

Wireless networks is essentially either infrastructure based mostly networks or infrastructure less networks. The infrastructure based mostly networks uses fastened base stations, that area unit answerable for coordinating communication between the mobile hosts (nodes). The unintentional networks falls underneath the category of infrastructure less networks, wherever the mobile nodes communicate with one another with none fastened infrastructure between them. an advert hoc network could be a assortment of nodes that don't believe a predefined infrastructure to stay the network connected. Therefore the functioning of Ad-hoc networks relies on the trust and co-operation between nodes. Nodes facilitate one another in conveyance of title data concerning the topology of the network and share the responsibility of managing the network. Therefore additionally to acting as hosts, every mobile node will perform of routing and relaying messages for different mobile node.

II. RELATED WORK

[1] Peer-to-peer networks square measure networks during which peers get together to perform a vital operate during a decentralised manner. All peers square measure each shoppers and suppliers of resources and might access one another directly while not negotiator peers. Compared with a centralized system, a peer-to-peer (P2P) system provides a straightforward thanks to mixture massive amounts of resources residing on the sting of web or in ad-hoc networks with a coffee price of system maintenance. P2P systems have attracted increasing attention from researchers recently, however they additionally mention some issues. Since peers square measure heterogeneous, some peers can be benevolent in providing services. Some can be buggy or malicious and can't give services with the standard that they advertise. Since there's no centralized node to function associate authority to observe and penalise the peers that behave badly, malicious peers have associate incentive to produce poor quality services for his or her profit as a result of they'll depart. Some ancient security techniques, like service suppliers requiring access authorization, or shoppers requiring server authentication, square measure used as protection from well-known malicious peers.

Fig1. Mobile ad-hoc network.

However, they can't forestall from peers providing variable-quality service, or peers that square measure

unknown. Mechanisms for trust and name will be wont to facilitate peers distinguish sensible from dangerous partners. This [1]paper describes a trust and name mechanism that permits peers to find partners WHO meet their individual needs through individual expertise and sharing experiences with different peers with similar preferences. In our model a peer builds 2 varieties of trust in another peer, say peer A and peer B respectively. The primary one is that the trust that peer A has in peer B's capability in providing services. Alternative is that the trust that peer A has in peer B's dependability in providing recommendations regarding other peers. Here the dependability includes 2 aspects:

Truthfulness – whether or not peers B is truthful in telling its data.

Similarity – whether or not peers B is comparable to peer A in preferences and ways that of deciding problems.

In the[2] future generation of wireless communication technology, there'll be a necessity for the fast readying of freelance mobile users. Substantial examples embody establishing survivable, dynamic,economical communication for emergency/rescue operations, military, and disaster relief effort networks. Such technology eventualities cannot believe centralized and arranged infrastructure, however are often formed as applications of MANET. A Mobile Ad Hoc Networks is associate autonomous assortment of mobile users that communicate over comparatively information measure affected wireless ties.

Since the nodes square measure movable, the constellation could modification apace and erratically over time. Technology is redistributed, wherever all network activity together with discovering the topology and delivering messages should be dead by the nodes itself, i.e., the routing practicality are going to be incorporated into mobile node. In [2] paper, associate approach has been planned to combat black-hole attack in AODV routing protocol. During this approach any node uses variety rules to illation regarding honesty of reply's sender. Activities of a node in a very network show its honesty. To participate in data transfer methodology, a node ought to demonstrate its honesty. Early of simulation, all nodes square measure able to transfer data; in order that they would like enough time to point its truth (Though every node square measure typically a control less one). If a node is that the first receiver of a RREP packet, it forwards packets to provide and initiates judgment methodology on regarding replier. The judgment method-logy is base on opinion of network nodes regarding replier. The activities of node data square measure logged by its neighbors table given in fig.3. These neighbors square measure requested to send their opinion one or two of node. Once a node collects all opinions of neighbors, it decides if the replier is also a malicious node. The selection is base on vary rules. The following rules used during this paper to measure regarding honesty of a node in network. This judgment is base on nodes square measure activity in network.

A. Existing system & disadvantages

There are two complementary categories of approaches that may safeguard tactical MANETs: prevention-based and detection based mostly approaches. One issue of those prevention-based approaches is that a centralized key management infrastructure is required, which cannot be realistic in distributed networks like MANETs. Additionally, centralized infrastructures are the most targets of rivals in battlefields. If the infrastructure is destroyed, then the total network could also be paralytic. Serving because the second wall of protection, detection-based approaches will effectively facilitate determine malicious activities. Though some wonderful work has been done on detection based mostly approaches supported trust in MANETs, observation in most approaches is simply accustomed assess the dependability of nodes, that don't seem to be within the vary of the observer node. Therefore, inaccurate trust values could also be derived.

III. PROPOSED SYSTEM

We have a tendency to projected the system with 2 observations one is direct and alternative one is indirect, in direct methodology every node will observe the behavior of alternative immediate nodes, and indirect model every node observes the knowledge regarding multi-hop node by the immediate trustworthy node. We'll use the history of the every immediate nodes behavior for direct observation. And name theme for indirect observation. By victimisation the projected trust management theme able to get the correct price and that we can avoid the misconduct nodes from the route. In our base model, the researchers have used the direct observation by overhearing the knowledge. This methodology is best in a number of the situations however this won't be sensible altogether alternative situations.

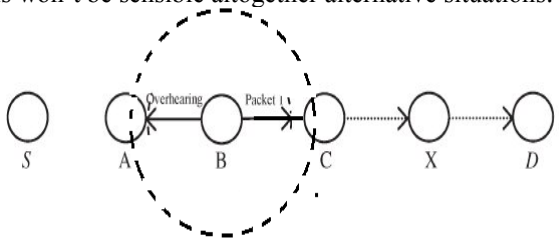

Fig.2. Overhearing technique.

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.

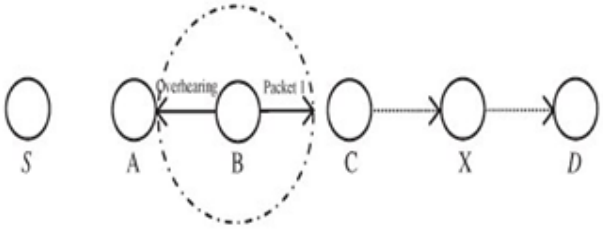

Fig.3. Overhearing method security problem.

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

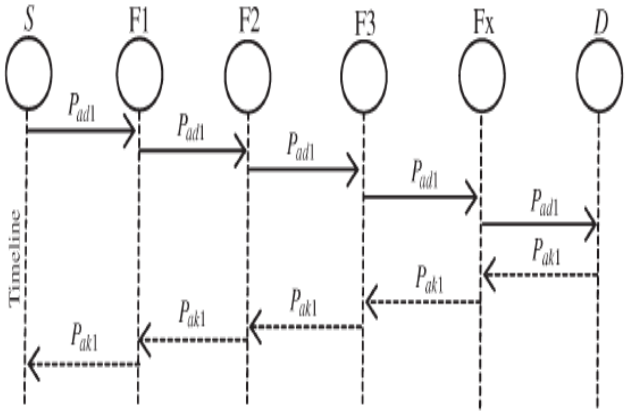

Fig.4. ACK based security implementation.

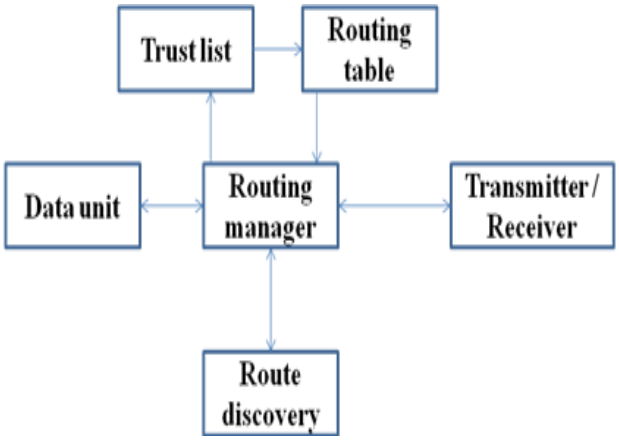

Fig.5. Block diagram.

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.

B. 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.

1. 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

2. 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 $\in$ table
         1. Ignore the message
      ii. If forwarder $\notin$Meli table
         1. For i$\in$ Meli table
            a. Updates "*i*" in RREQ
         2. If current node == destination of the pkt
            a. RREQ $\Rightarrow$RREP
               i. Update the reverse route info
            b. Send to source
         3. If current node $\neq$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

3. 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*" ∈ OREQ list
      i. If "*i*" ∈Meli 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.

4. 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

IV. RESULT ANALYSIS

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.

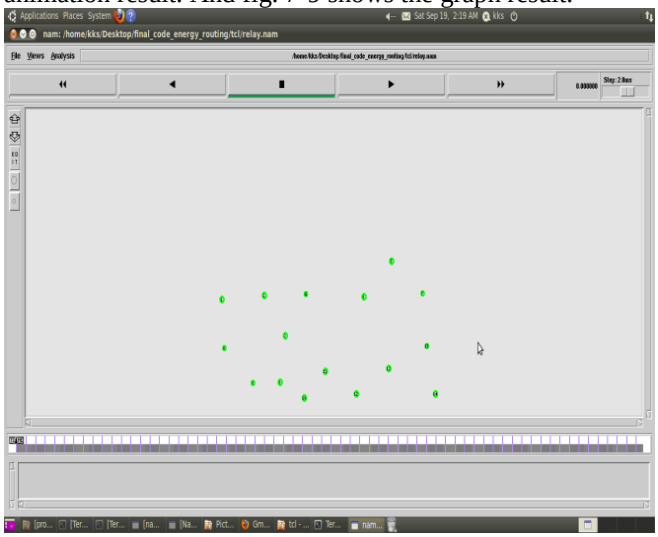

Fig.6. Network setup.

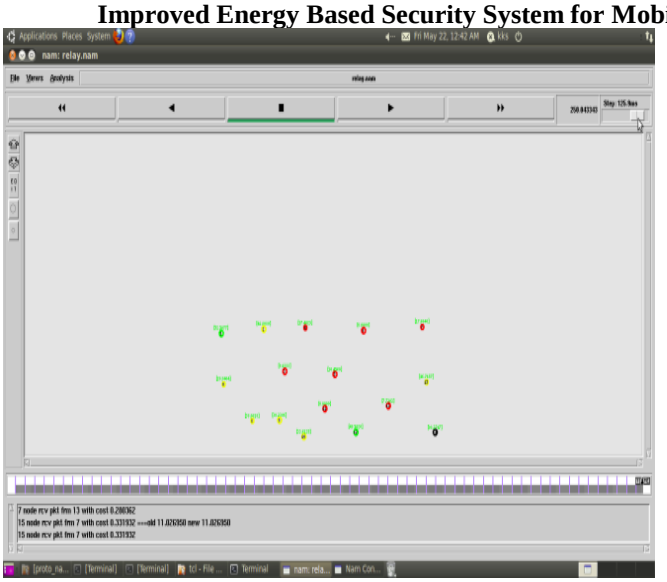

Fig.7. Node failure due to attack.

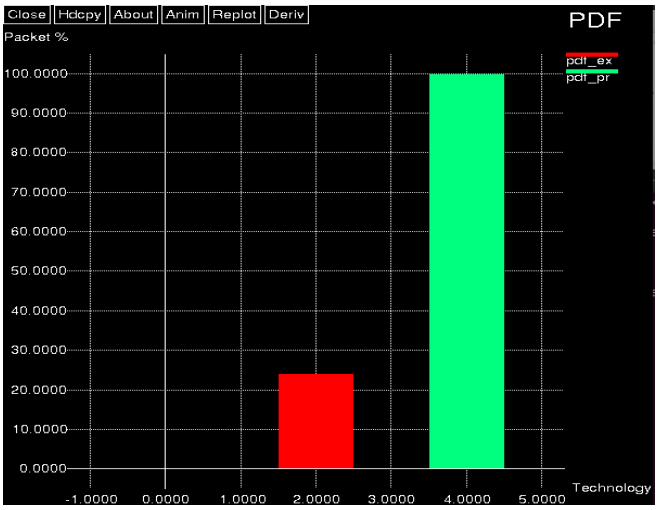

Fig.8. Packet delivery comparison (Enhanced system provides more packet delivery {green} than existing work).

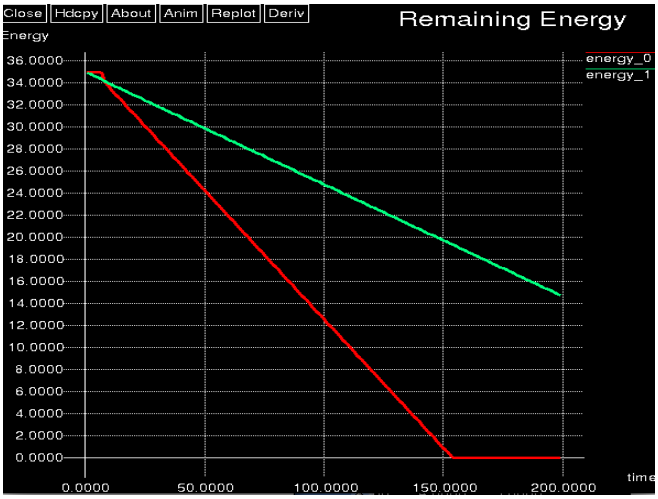

Fig.9. Energy comparison (our method provides high energy saving {green}).

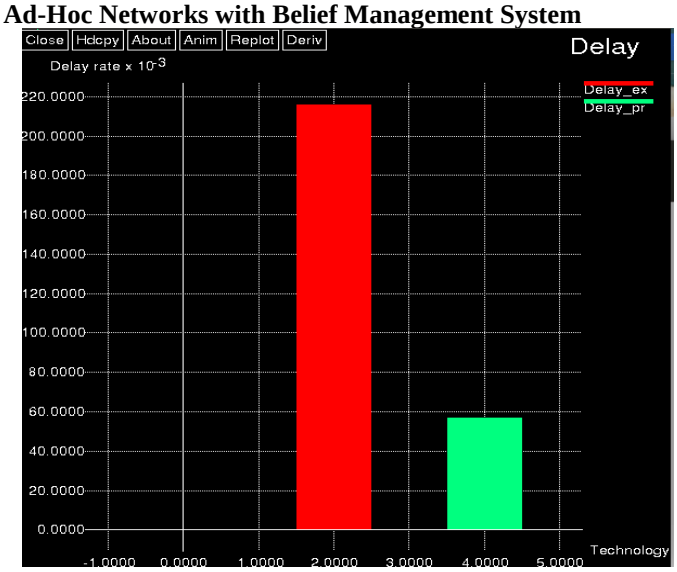

Fig.10. Delay comparison (our method provides less delay {green}).

V. 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.

VI. REFERENCES

[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.
[9] 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.

Author's Profile:

K.Kartheeka has completed her B.Tech in ECE Department from Methodist College of Engineering and technology, OU Hyderabad. Presently she is pursuing her Masters in Electronics and Communications from Vardhaman College of Engineering, Shamshabad, Hyderabad, India.

Mrs.V. Harini received the M.TECH degree from VIT University. She is the Assistant professor in the Department of Electronics and Communication Engineering. She has 5 years of teaching experience.

Mr.S.Srinivas has completed his B.TECH (ECE) from JNTU 2004 and M.TECH (WMC) from JNTU 2010. He has 9 years of teaching experience. Currently working as an Assistant Professor and H.O.D of WMC in Vardhaman College, Hyderabad, T.S, India.