International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2163
Volume 1 Issue 5 (June 2014) http://ijirae.com

Requisite Trust Based Routing Protocol for WSN

Vasudha N
M.Tech Student,
Sri Venkateshwara College of Engineering, Bangalore

Dr. Pritam Gajkumar Shah
Professor Department of E&C
Sri Venkateshwara College of Engineering Bangalore

ABSTRACT-- A mobile ad-hoc network (MANET) is an infrastructure less network of mobile devices connected by wireless links. To secure a MANET in colluding nodes environment, the proposed work aims to detect and defend colluding nodes that causes internal attacks. In order to achieve this, the work focuses on the novel algorithm of trust computation and route detection that detects colluding nodes, without message and route redundancy during route discovery by using Requisite Trust based Secure Routing Protocol (RTSR). The trust will be calculated in local forwarding nodes, which are used to discover the route. The trust values from one hop neighbors are used to calculate the single trust value for each node using the constant normalization concept. Route discovery and trust information will be stored in fixed cluster head (CH).

Keywords: Trust based routing, wireless sensor networks (WSNs), LEEACH.

I. INTRODUCTION

Placement of nodes in Wireless Sensor Network (WSNs) is often massive and LEEACH. Topology control algorithms focus in lowering the initial network topology, by reducing active nodes and links, thus saving resources and increasing network lifetime. Currently, most algorithms and schemes in WSNs, construct shared, core-based trees, with the sink as a root for this purpose. In this project, we study whether trees that initiate from each source, called source-based trees, can assist in this purpose and provide, under specific circumstances, an efficient topology control solution.

Massive and LEEACH placement of sensor nodes on a monitored field renders node communication a difficult task to be achieved. Interference, congestion, and routing problems are possible to arise at any point in such networks. Routing challenges in WSNs stem from the unique characteristics of these networks, such as limited energy supply, limited computing power, and limited bandwidth on the wireless links, which impose severe restrictions on the design of efficient routing protocols. According to theory, a number of routing challenges and design issues like, among others, node placement and energy consumption, can affect routing process in WSNs.

Thus, topology control, in conjunction with routing challenges, becomes an important issue that has to be carefully considered in order to achieve proper network operation. Generally, congestion control algorithms in WSNs employ two methods in order to control and avoid congestion. The first method is called traffic control and the second resource control. Algorithms that employ the traffic control method, adjust the rate with which sources inject traffic to the network in order to control congestion. On the other hand, resource control algorithms employ redundant nodes, which are not in the initial path from source to sink, in the process of forwarding data. Thus, algorithms that employ this method do not control the data rate of the sources but the paths though which the data flows. According to studies traffic control algorithms are not affected by different node placements, while according to the same studies resource control algorithms are significantly affected. Different node placements create a variable number of paths which are important for the proper operation of these algorithms. Placement of nodes in Wireless Sensor Network (WSNs) is often massive and LEEACH. Permitting all nodes to transmit concurrently without any control will result in high interference, high energy consumption, and reduced network lifetime.

II. SECURITY IN WIRELESS AD-HOC NETWORKS

Security is an important thing for all kinds of networks including the Wireless Networks. It is obviously to see that the security issues for Wireless sensor Networks are difficult than the ones for fixed networks. This is due to system constraints in mobile devices as well as frequent topology changes in the Wireless networks. Here, system constraints include low-power, small memory and bandwidth, and low battery power. Mobility of relaying nodes and the fragility or routes turn Wireless Ad-hoc Network architecture into highly hazardous architectures. No entity is ensured to be present at every time and it is then impossible to rely on a centralized architecture that could realize network structure or even authentication. The people who consider the Mobile Ad hoc Networks are not a flawed architecture, while we cannot see it used in practice is only because most of its applications are in military are totally wrong. It is true that Mobile Ad hoc Networks come from the military. But perhaps those persons forgot one of the most important things: the Security! Everybody knows that the core requirement for military applications dealing with trust and security! That is to say, security is the most important issue for ad hoc networks, especially for those security sensitive applications. Security is difficult to implement because of the networks constrains and the rapidly topology changes. After investigation, we found that there are two kinds of security related problems in the Mobile Ad-hoc Networks.

One is the attacks based on the networks which are just similar to the Internet, the other is Fault Diagnoses. Fault Diagnoses algorithm is used to pick out the faulty nodes and at the same time remove the node from the whole networks. This process should be real-time as to guarantee the performance of the whole networks. In order to solve the fault diagnoses problem, many fault diagnoses algorithms were bring out. After carefully surveying the existing algorithm today, one can found that they

cannot correctly diagnose faulty node with the presence of the changing of the network topology during the process of diagnosis, and these algorithms are analyzed with repetitious diagnosis for all the mobile hosts and cause the great system overhead due to the transmission of diagnosis messages by means of flooding throughout the whole networks. While the topology of Mobile Ad-hoc Networks changes from time to time, then we cannot use this kind of Fault Diagnoses Algorithm to solve the questions. Therefore, we can see that the current fault diagnosis algorithms cannot solve the fault diagnosis problem.

As for the networks attacks, there are several factors of security that we should consider.

1. *Availability* ensures the survivability of network services despite denial of service attacks.
2. *Confidentiality* ensures that certain information is never disclosed to unauthorized entities.
3. *Integrity* guarantees that a message being transferred is never corrupted.
4. *Authentication* enables a node to ensure the identity of the peer node it is communicating with. Yet, active attacks might allow the adversary to delete massages, to modify messages, and to impersonate a node, thus violating availability, integrity, authentication, and non-repudiation. Although that many security-related researches have been done to this problem, we could see that Mobile Ad hoc networks are inherently vulnerable to security attacks. While, on the other hand, it is said that the main applications of MANET are in military and emergency, all these applications are security-sensitive.

III. PROBLEM STATEMENT

The increasing demand for wireless mobile communication, especially in situations where traditional infrastructure communication networks do not exist or were destroyed, has encouraged the appearance of the infrastructure less Mobile Ad hoc Networks commonly referred to as (MANETs). MANETs enable the communication of mobile (nodes) without the aid of any physical central point of communication (e.g. neither a base station nor central office involved). The nodes in MANETs may be mobile devices like: laptops, palmtops or mobile-phones. MANETs are multi-hop, self-organized and decentralized networks. The dynamic nature of MANETs provides many challenges that require extensive research in order to provide a satisfying performance to their mobile users. The security is the most important concern in a MANET network.

IV. EXISTING SYSTEM

A wireless sensor network (WSN) often contains hundreds or thousands of sensor nodes equipped with sensing, computing, and communication devices such as short-range communication devices over wireless channels. These nodes may be distributed over a large area; e.g., WSNs can do area monitoring for some phenomenon of interest. In such an application, the main goal of the WSN is to collect data from the environment and send it to a sink node. The previous approach does not take route into consideration the security check while doing a route discovery process. The LEEACH algorithm of the WSN network was used in the unicasting of the packets and it was observed that the LEEACH maintains local topology in both normal nodes and cluster heads. Hence a lot of communication is needed between the nodes. This increases the energy consumption, Power consumption, number of hops and end to end delay.

V. PROPOSED SYSTEM

In this project RTSR protocol, has proposed the low secure nodes detection and defence mechanism by using both cluster-based approach and trust-based route discovery through every node in a MANET. The route redundancy and message redundancy will be reduced by broadcasting the packets. Using piggybacking bit for trusts the lesser bandwidth consumption will be maintained and the broadcast storm problem will be reduced. The project divides the nodes into compartments like trains called as clusters and one special node is known as cluster head. The forward nodes selection is done based on the calculation of trust and efficient route is discovered based on maximum trust level.

5.1 SYSTEM ARCHITECTURE

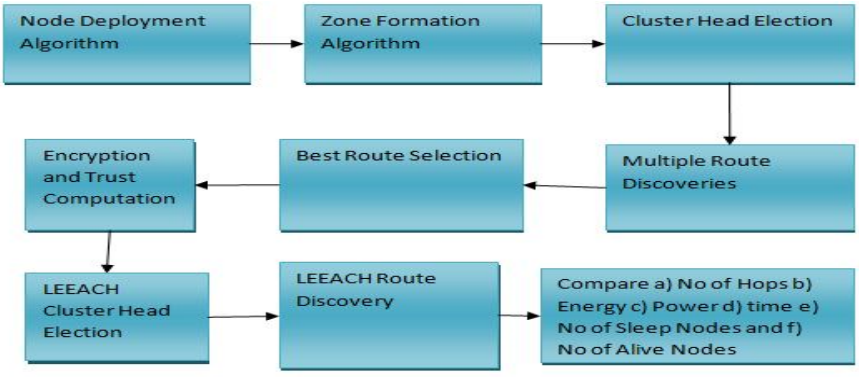


Fig5.1: System Architecture

Figure shows the system architecture diagram for the TRUST Based routing algorithm.

1. **Node Deployment Algorithm**
   This algorithm is responsible for deployment of nodes in a particular area
2. **Zone Formation Algorithm**
   Zone Formation algorithm divides the entire are into multiple zones. Each zone having a set of nodes in its zone. This is the algorithm which is responsible for deploying the nodes. The entire area is divided into zones with each zone bounded with the limits with some xmin and xmax. The y region is bounded within the limits ymin and ymax. Each zone is allocated a set of nodes.
3. **Cluster Head Election**
   This algorithm is used to elect the zone leader by computing distance value .The distance value is computed per zone for all nodes and whichever node has minimum value of distance becomes the zone leader.
4. **Multiple Route Discovery**
   This is used to find multiple routes from source node to destination node
5. **Best Route Selection**
   This algorithm is responsible for selecting the best route which has the maximum trust.
6. **LEEACH Cluster Head**
   This algorithm elects the cluster head LEEACH.
7. **LEEACH Route Discovery**
   The LEEACH Route Discovery algorithm is used to discover the path from the source node to the destination node.
8. **Hops Comparison**
   This is defined as the number of intermediate nodes between the source nodes to destination node.
9. **Energy Comparison**
   This is defined as the energy consumption for transferring the control packets between the source nodes to destination node. It is defined by the equation

   $$TE_c = \sum_{i=1}^{N_l} E_c(i)$$

   Where, $N_l = Number\ of\ Links$

   $$E_c = 2 * E_{tx} + E_{amp}\ d^{\delta}$$

   Where,

   $E_{tx} = Energy\ required\ to\ transmit\ control\ packet$

   $E_{amp} = Energy\ required\ for\ amplificat\ ion$

   $d = dis\tan ce\ between\ the\ nodes$

   $\delta = attunuatio\ n\ factor$
10. **Power Comparison**
    This entity is used to do the power comparison between the two algorithms. The total power consumption of the route is defined as

    $$TP_c = \sum_{i=1}^{N_l} P_c(i)$$

    Where, $N_l = Number\ of\ Links$

    And $Pc(i) = PowerConsu\ med\ across\ link\ i$ is given by

    $$P_c = \frac{P_t}{1 + d^{\gamma}}$$

    $P_t = power\ required\ for\ transmissi\ on$

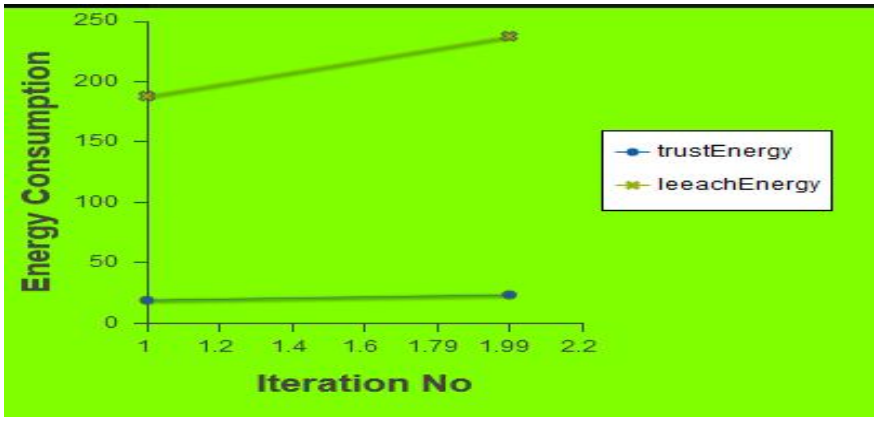
    $d = dis\tan ce\ between\ the\ nodes$

    $\gamma = environmen\ t\ factor$

    $0 \le \gamma \le 1$

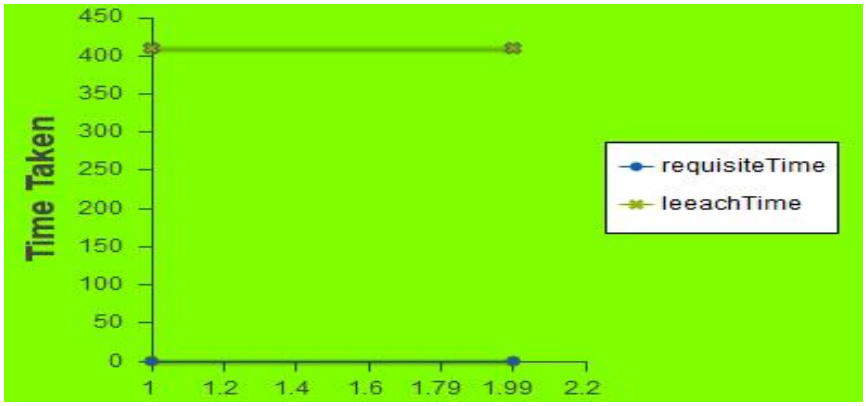
    The environment factor values for the different environments in the WSN network are

Environment Factor	Value
Standard	0.5
Rainy	0.07
>42	0.8
<30	0.0654



11. End to End Delay or Route Discovery Time

The end to end delay is the time taken for a control packet to traverse from source node to destination node and come back.



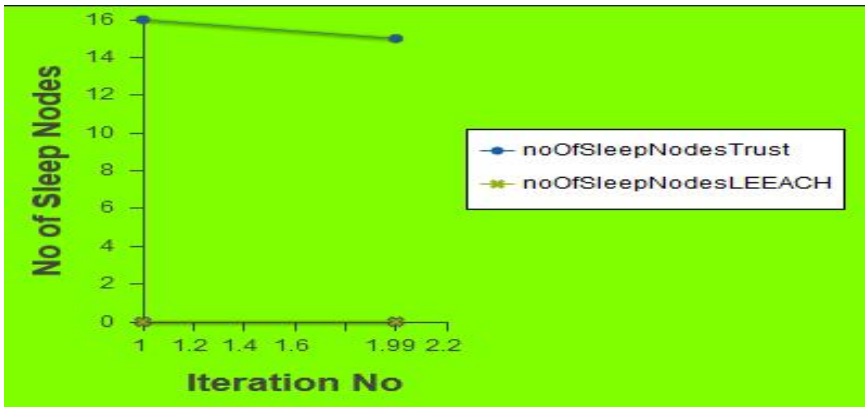
$RDT = t_{stop} - t_{start}$

$t_{stop} = Time \ \ at \ \ which \ \ RRPLY \ \ is \ \ recieved \ \ at \ \ the \ \ source \ \ node$

$t_{start} = Time \ \ at \ \ which \ \ RREQ \ \ is$ int $iated \ \ at \ \ the \ \ source \ \ node$

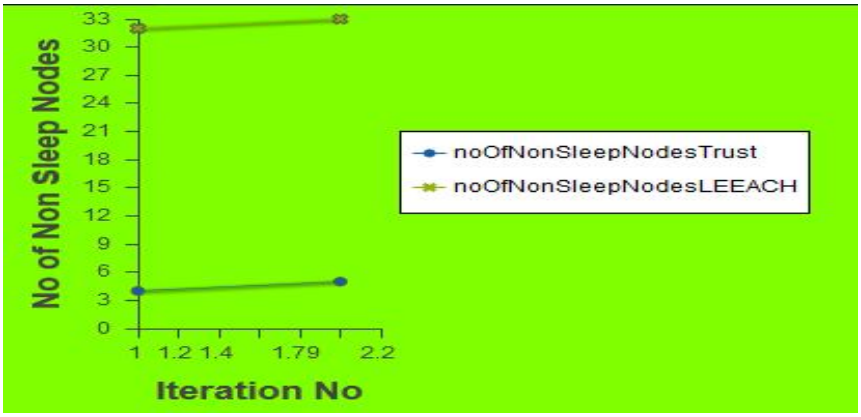
12. Sleep Nodes

This is the nodes which have not participated in routing



13. Non Sleep Nodes

These are the nodes which participated in routing



VI. CONCLUSION AND FUTURE SCOPE

Wireless sensor networks (WSNs) are large collections of small sensor devices that can be an effective tool for collecting data from various environments. Each sensor sends its data to Base Station (BS), and finally BS sends these data to end user. Clustering is considered as an effective approach to provide better data gathering and scalability for large sensor networks. In this project we demonstrate efficient way of routing with respect to trust levels which increases the overall security of the network. We take 3 different algorithms for computation of trust namely direct, eigen and dempster and prove that the dempster is the best algorithm because it takes both control and data packets into consideration. The network routing algorithm can be future improved by bringing into picture the concept of Friendship Routing by forming the friendship routing which can be used to deliver packets to the destination thereby decreasing the power consumption even more. The network lifetime and processing time can be taken as the future parameters.

REFERENCES

[1] N. Bulusu, J. Heidemann, and D. Estrin, GPS-less Low Cost Outdoor Localization for Very Small Devices, IEEE Personal Communications Magazine, October 2000.
[2] A. Cerpa, J.Wong, L. Kuang, M. Potkonjak, and D. Estrin, Statistical Model of Lossy Links in Wireless Sensor Networks, IPSN, April 2005.
[3] J. Elson, L. Girod, and D. Estrin, Fine-Grained Network Time Synchronization Using Reference Broad-casts, OSDI, December 2002.
[4] S. Ganeriwal, R. Kumar, and M. Srivastava, Timing-sync Protocol for Sensor Networks, ACM SenSys, November 2003.
[5] T. He, J. Stankovic, C. Lu and T. Abdelzaher, A Spatiotemporal Communication Protocol for Wireless Sensor Networks, IEEE Transactions on Parallel and Distributed Systems, to appear.
[6] T. He, C. Huang, B. Blum, J. Stankovic, T. Abdelzaher, Range-Free Localization and Its Impact on Large Scale Sensor Networks, ACM Transactions on Embedded Computing System, to appear.
[7] T. He, S. Krishnamurthy, J. Stankovic, T. Abdelzaher, L. Luo, T. Yan, R. Stoleru, L. Gu, G. Zhou, J. Hui and B. Krogh, VigilNet: An Integrated Sensor Network System for Energy Efficient Surveillance, ACM Transactions on Sensor Networks, to appear.
[8] T. He, P. Vicaire, T. Yan, L. Luo, L. Gu, G. Zhou, R. Stoleru, Q. Cao, J. Stankovic, and T. Abdelzaher, Real-Time Analysis of Tracking Performance inWireless Sensor Networks, IEEE Real-Time Applications Symposium, May 2006.
[9] T. He, P. Vicaire, T. Yan, Q. Cao, L. Luo, L. Gu, G. Zhou, J. Stankovic, and T. Abdelzaher, Achieving Long Term Surveillance in VigilNet, Infocom, April 2006.
[10] J. Hill, R. Szewczyk, A, Woo, S. Hollar, D. Culler, and K. Pister, System Architecture Directions for Networked Sensors, ASPLOS, November 2000.
[11] C. Intanagonwiwat, R. Govindan, and D. Estrin, Directed Diffusion: A Scalable Routing and Robust Communication Paradigm for Sensor Networks, Mobicom, August 2000.
[12] B. Karp, Geographic Routing for Wireless Networks, PhD Dissertation, Harvard University, October 2000.
[13] B. Karp and H. T. Kung, GPSR: Greedy Perimeter Stateless Routing for Wireless Sensor Networks, IEEE Mobicom, August 2000.
[14] P. Levis and D. Culler, Mate: A Tiny Virtual Machine for Sensor Networks, Int. Conf. on Architectural Support for Programming Languages and Operating Systems, October 2002.
[15] J. Liu, M. Chu, J.J. Liu, J. Reich and F. Zhao, State-centric Programming for Sensor and Actuator Network Systems, IEEE Pervasive Computing, October 2003.

