IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 10, October 2017

Enhanced Robust Ad-hoc Sensor Routing (RASeR) Protocol with Trust Authentication Scheme for Wireless Sensor Networks

N. Suresh[1], S. Anandhan[2]

Assistant Professor, Department of Computer Science & Applications, Mahendra Arts & Science College (Autonomous), Kalipatti, Namakkal, Tamil Nadu, India[1]

M. Phil Scholar, Department of Computer Science & Applications, Mahendra Arts & Science College (Autonomous), Kalipatti, Namakkal, Tamil Nadu, India[2]

Abstract: 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. The proposed analysis shows significant improvement in packet delivery ratio of AODV in the presence of attacks, with marginal rise in control traffic overhead. The forwarding technique used inherently takes advantage of route diversity, which is designed to utilize multiple paths simultaneously, such that if one route fails there is another still active to deliver the packet. This makes the protocol very dependable in terms of packet delivery and very robust to link failure.

Keyword: Raser Protocol, Routing, MAC, AODV, EAODV.

I. INTRODUCTION

Wireless sensor networks have recently come into prominence because they hold the potential to revolutionize many segments of our economy and life, from environmental monitoring and conservation, to manufacturing and business asset management, to automation in the transportation and health care industries. The design, implementation, and operation of a sensor network requires the confluence of many disciplines, including signal processing, networking and protocols, embedded systems, information management and distributed algorithms. Such networks are often deployed in resource-constrained environments, for instance with battery operated nodes running un-tethered.

Mobile Ad-Hoc Network (MANET) is a collection of autonomous nodes that form a dynamic purpose-specific multi hop radio network in a decentralized fashion. MANETs, being cost-effective and quick to install, find many applications in military environments, emergency and rescue operations, civilian environments and education.

Many researchers have come up with many routing protocols in MANET, as described. However, AODV outperforms DSR in more demanding situations. In these applications data have significant role. But, MANETs are often vulnerable to security attacks that lead to unauthorized access and use, disclosure, disruption, modification or destruction of data.

Moreover, packet dropping attacks are inevitable in such hostile environments. Further, MANET routing protocols inherently trust all participants. The naive trust allowsmalicious nodes to paralyze the network by inserting false routing updates, or advertising incorrect routing information.

Several AODV routing protocol related attacks in MANET have been described. A malicious node may fabricate, modify, intercept or interrupt packets. As an example, a malicious node advertises a route to a destination by fabricating route reply (RREP) message. By doing so the attacker attracts the traffic towards itself, as in black hole attacks. A node with malicious intent modifies RREP messages to misguide the node to send data packets to attackers, as in misrouting attacks. Colluding nodes with malicious intent may reveal intercepted RREP messages among themselves to instigate a collaborative attack such as wormhole attack.

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 10, October 2017

A malicious node may interrupt RREP messages by dropping the RREP control packets. Counter measure for all such attacks that are based on RREP messages is not feasible only by monitoring RREP messages. However, by listening promiscuously to the neighboring node's transmission and cross-correlation between various monitored traffic can reveal the true behavior of neighboring nodes to thwart security threats in MANET. Further, discovering a trustworthy path in MANET is a real challenge.

MANETs are self-creating, self-organizing, self-administrating and do not require deployment of any kind of fixed infrastructure. They offer special benefits and versatility for wide range of applications in military (e.g., battlefields, sensor networks etc.), commercial (e.g., distributed mobile computing, disaster discovery systems, etc.), and educational environments (e.g., conferences, conventions, etc.), where fixed infrastructure is not easily acquired. With the absence of pre-established infrastructure (e.g., no router, no access point, etc.), two nodes communicate with one another in a peer-to-peer fashion. Two nodes communicate directly if they are within the transmission range of each other. Otherwise, the nodes communicate via a multihop route. To find such a multi-hop route, MANETs commonly employ on demand routing algorithms that use flooding or broadcast messages.

II. LITERATURE REVIEW

Konrad Lorincz, David J. Malan [1] describe Sensor networks, a new class of devices, have the potential to revolutionize the capture, processing, and communication of critical data for use by first responders. Sensor networks consist of small, low-power, and low-cost devices with limited computational and wireless communication capabilities. They represent the next step in wireless communication's miniaturization, and their power and size make it feasible to embed them into wearable vital sign monitors, location-tracking tags in buildings, and first responder uniform gear. Sensor nodes' extreme resource limitations represent new challenges in protocol design, application development, and security models.

The authors developed CodeBlue [4], a common software infrastructure, to address these challenges. CodeBlue integrates sensor nodes and other wireless devices into a disaster response setting and provides facilities for ad hoc network formation, resource naming and discovery, security and in network aggregation of sensor-produced data. They designed CodeBlue for rapidly changing, critical care environments. To test it, they developed two wireless vital sign monitors and a PDA-based triage application for first responders. Additionally, they developed MoteTrack, a robust radio frequency (RF)–based localization system, which lets rescuers determine their location within a building and track patients. Although much of their work on CodeBlue is preliminary, their initial experience with medical care sensor networks raised many exciting opportunities and challenges.

Jamal N. Al-Karaki Ahmed E. Kamal [2] describe Wireless Sensor Networks (WSNs) consist of small nodes with sensing, computation, and wireless communications capabilities. Many routing, power management, and data dissemination protocols have been specifically designed for WSNs where energy awareness is an essential design issue. The focus, however, has been given to the routing protocols which might differ depending on the application and network architecture. In this paper [11], they present a survey of the state-of-the-art routing techniques in WSNs.

They first outline the design challenges for routing protocols in WSNs followed by a comprehensive survey of different routing techniques. Overall, the routing techniques are classified into three categories based on the underlying network structure: flat, hierarchical, and location-based routing. Furthermore, these protocols can be classified into multipath-based, query-based, negotiation-based, QoS-based, and coherent-based depending on the protocol operation. They study the design tradeoffs between energy and communication overhead savings in every routing paradigm. They also highlight the advantages and performance issues of each routing technique.

Xiaoxia Huang, Hongqiang Zhai and Yuguang Fang [3] describe a wireless sensor networks, path breakage occurs frequently due to node mobility, node failure, and channel impairments. It is challenging to combat path breakage with minimal control overhead, while adapting to rapid topological changes. Due to the Wireless Broadcast Advantage (WBA), all nodes inside the transmission range of a single transmitting node may receive the packet, hence naturally they can serve as cooperative caching and backup nodes if the intended receiver fails to receive the packet. In this paper [16], they present a distributed robust routing protocol in which nodes work cooperatively to enhance the robustness of routing against path breakage. They compare the energy efficiency of cooperative routing with non cooperative routing and show that their robust routing protocol can significantly improve robustness while achieving considerable energy efficiency.

Wireless sensor networks are envisioned to be essential to many applications and will impact their daily life significantly. In many application scenarios, wireless sensor networks must be mobile. As an example, in wildlife

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 10, October 2017

monitoring or environmental study, sensors are cast in the field as well as are equipped on free-ranging animals to be monitored. In mobile wireless networks, path breakage occurs more frequently due to channel fading, shadowing, interference, node mobility as well as power failure. When a path breaks, rerouting or alternative routing may be necessary and should be carried out promptly. Otherwise, packet loss and large delay would occur. Different types of routing protocols have been proposed for mobile wireless ad hoc networks.

However, they are not suitable for highly dynamic topologies, especially for energy and computation capability constrained sensor nodes. Therefore, prompt path recovery, energy efficiency and robustness are highly preferred characteristics for routing protocols in mobile wireless sensor networks. As a node on the original path moves, the set of guard nodes changes accordingly. So the effective guard node set is also dynamic in mobile wireless networks. The dynamic change comes from two scenarios. One is due to the movement of intended nodes.

G. Santhosh Kumar, Vinu Paul M V, G. Athithan and K Poulose Jacob [4] describe a wireless sensor networks, the routing algorithms currently available assume that the sensor nodes are stationary. Therefore when mobility modulation is applied to the wireless sensor networks, most of the current routing algorithms suffer from performance degradation. The path breaks in mobile wireless networks are due to the movement of mobile nodes, node failure, channel fading and shadowing. It is desirable to deal with dynamic topology changes with optimal effort in terms of resource and channel utilization. As the nodes in wireless sensor medium make use of wireless broadcast to communicate, it is possible to make use of neighboring node information to recover from path failure.

Cooperation among the neighboring nodes plays an important role in the context of routing among the mobile nodes. This paper [17] proposes an enhancement to an existing protocol for accommodating node mobility through neighboring node information while keeping the utilization of resources to a minimum.

Jaideep Lakhotia, Rajeev Kumar [5] describe a Mobile Wireless Sensor Network is having mobile nodes in the network. Both the sensor nodes and mobile sink can be mobile or there can be mixed sensor nodes i.e. mobile as well as static sensor nodes in the network based on the application requirements. Routing in mobile wireless sensor network poses research issues as nodes are mobile, so it needs to send the data according to the routing protocol while it is moving. So the routing protocols have been proposed considering mobile nodes in the network focusing on research issues like packet loss, energy consumption, and delay. In this paper [21], the cluster based routing protocols that have been proposed for mobile wireless sensor network are discussed and comparison is done among them.

III. METHODOLOGY

A. RASER PROTOCOL

Multi-radio wireless mesh networks need new routing metrics which can find the best routes using minimum end-to-end delay and least interference to improve the performance. Additionally, the routing metric should estimate the delay considering contention delay and interference using a combination of interference models. To address this, new metric called P-IDA is proposed which is based on 802.11 DCF basic access mechanism.
The P-IDA metric estimates the link quality in terms of delay, including transmission and contention delay, inter-flow interference using logical as well as physical interference model and intra-flow interference. In addition, as the link quality estimation is based on chosen transmission rate, the joint approach to routing metric computation and rate adaptation is required.

Delay Based Rate Adaptation (DBRA) mechanism based on the delay component of the P-IDA metric is proposed. The unique feature of the design is that, the link quality parameters are estimated using a passive mechanism which minimizes the control overhead. The joint approach is implemented in OLSR for multi-radio mesh networks by accessing parameters from PHY, MAC and network layers and estimating link quality based on the chosen rate.

- In general, the above reputation based schemes are based on number of packets dropped and forwarded as monitored by the neighbors.
- Most of the schemes completely isolate the malicious nodes thereby preventing them to recover.
- The existing system also addressed the limitations of blind flooding and proposed solutions to provide efficient flooding.
- However, because of the problem of finding a subset of dominant forwarding nodes in Wireless Mesh Networks , all the work about efficient flooding has been directed to the development of efficient heuristics that select a sub-optimal dominant set with low forwarding overhead.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 10, October 2017

B. TRUST BASE EAODV PROTOCOL

Trust embedded AODV and its trust model, proposed counter attacks selfish nodes in MWSN. In this, trust evaluation of a node is based on confidence level and forwarding ratio. Forwarding ratio of a node is the ratio of actually forwarded upon requested for forward, and the forwarding ratio weighted by packet size is considered as confidence level. The received forwarding ratio and confidence level from the neighbors contribute towards overall trust evaluation on a node.

The Trust base AODV includes this trust in its rebroadcasted RREQ packets to counter attack malicious nodes in the Wireless Mesh Networks. It does not allow any intermediate node to send route reply. The scheme presented in is based on incentives and penalties depending on the node behavior. In this, route trust is computed as the ratio of the number of packets received at the destination to the number of packets forwarded by a node on that route. Node trust is computed based on the difference between observed route trust value and advertised route trust value.

- The proposed system shows that EAODV and AODV 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 EAODV and AODV.
- In addition, the new system shows that EAODV is best suited for networks where movement of the nodes is moderate and AODV 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.

The proposed system 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 MWSN s to deal with misbehaving nodes in discovering trustworthy path. In addition two new enhancement techniques to reduce route request broadcast for reactive ad hoc routing protocols are proposed; (ii) Implementation of Enhanced Ad-hoc On-demand Distance Vector routing (EAODV) for moderate speed of node movement (iii) Implementation of Adaptive AODV (AAODV) which automatically switches over between EAODV1 and EAODV2 based on the mobility of the nodes.

C. ROUTING PROCESS

a) **TRUST BASED ROUTING PROTOCOL**

The proposed trust based routing protocol in the Wireless Mesh Networks architecture, with the help of an example, as shown in Fig.3.1. The WSN 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).

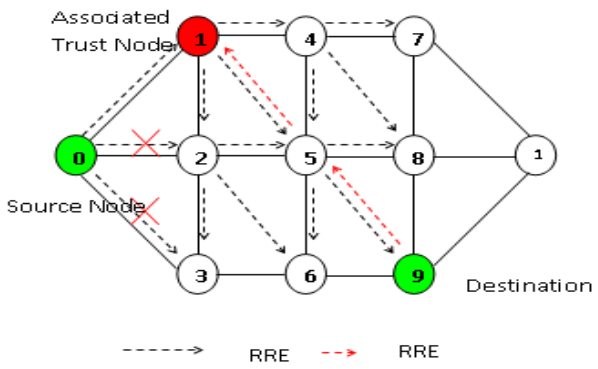

Fig 3.1(a). Trust based routing: Route Request (RREQ) and Route Reply (RREP)

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.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 10, October 2017

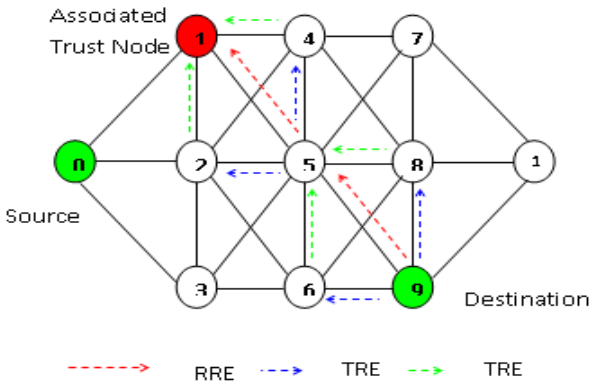

Fig 3.1 (b) Route Reply (RREP), Trust Request (TREQ) and Trust Reply (TREP)

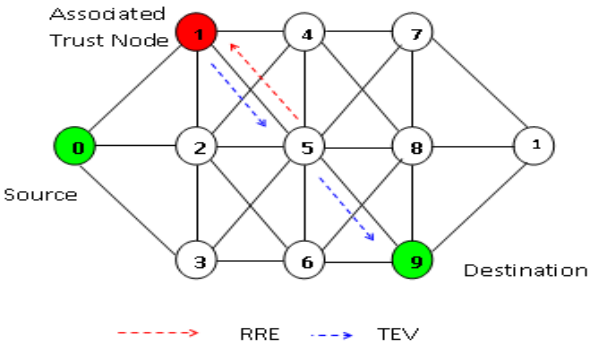

Fig 3.11(c) Route Reply (RREP) and Trust Evaluate (TEVAL)

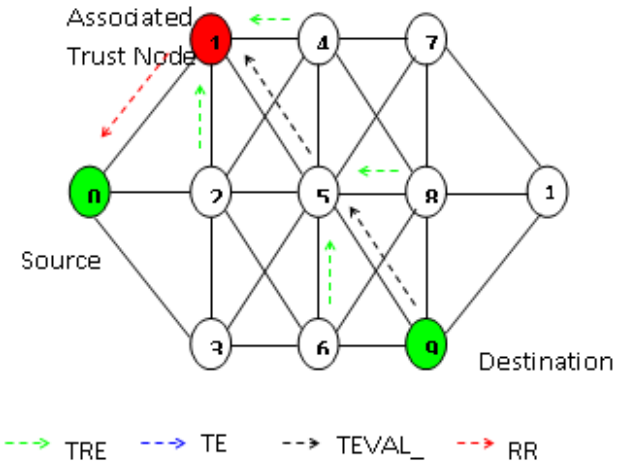

Fig 3.1(d) Trust Evaluate Acknowledgment (TEVAL ACK) and Route Reply (RREP)

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.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 10, October 2017

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

IV. EXPERIMENTAL RESULTS

PARAMETER	VALUE
Simulation tool	Ns2
Simulation Time	100ms
Number of Nodes	50
Routing Protocol	ADOV
Performance Metrics	Execution Time Analysis

Table 4.1 Environment creation setup

Due to the wide diversity of mesh nodes, the time consumption of mesh nodes varies greatly. For passive wireless mesh node, power consumption is negligible in comparison to other devices on a frequent mesh node wireless mesh node. On the other hand, for active mesh nodes (such as sonar, soil and gas mesh nodes) time consumption can be significant. Each wireless mesh node can include several node, and each of these mesh node typically has its own energy consumption characteristics and, in some cases, its own sampling frequency. In a mesh node, i, will have the following sensing time consumption.

$$E_{Tm}=Vdc*Ii*Tk$$

where T_i is the time required for obtaining a single sample from mesh node i and I_i is the current draw of mesh node i. T_i depends on the start-up (T_s), response (T_r) and measurement (T_m) times of the mesh node. As T_m is small in comparison to T_s and T_r for most mesh node, we consider only T_s and T_r in calculating T_i. Consider the value $\mathbf{V_{dc}= 0.6}$

MESH NODE (i)	I_i (sec)	T_m (ms)		T_i (ms)	E_{Tm} (ms)
		T_s (ms)	T_r (ms)		
L1	0.10	0.015	0.017	0.05	0.003
L2	0.20	0.025	0.029	0.07	0.006
L3	0.30	0.035	0.044	0.06	0.011
L4	0.40	0.042	0.046	0.08	0.016
L5	0.50	0.050	0.063	0.08	0.024
L6	0.60	0.064	0.076	0.13	0.034
L7	0.70	0.076	0.089	0.14	0.043
L8	0.80	0.081	0.095	0.15	0.058

Table 4.2 Execution Time Analysis-ADOV– EADOV

The startup time (T_s) is the time required for a mesh node to reach the ready state after time is engaged, upon which the mesh node can give the correct value. It is a well-known factor in the time management of mesh nodes. If a sensing task does not wait for the T_s after the micro controller unit (MCU) requests the mesh node to turn on, the task will receive the wrong value. T_s varies significantly between mesh node types.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 10, October 2017

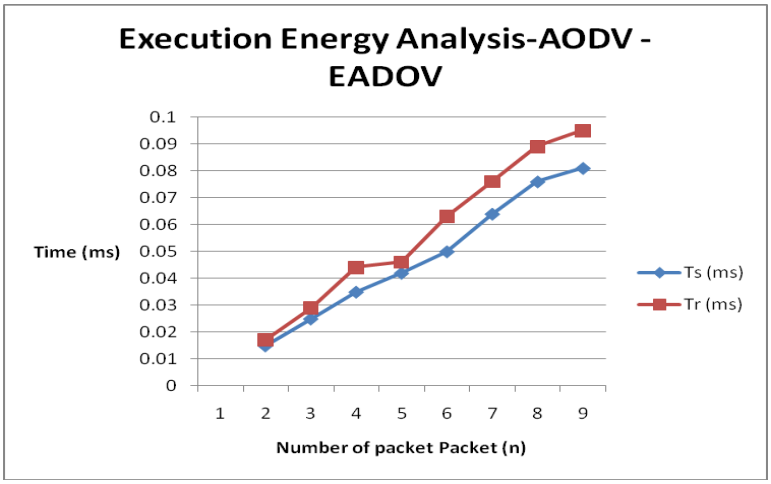

Fig 4.1 Execution Energy Analysis-AODV-EAODV

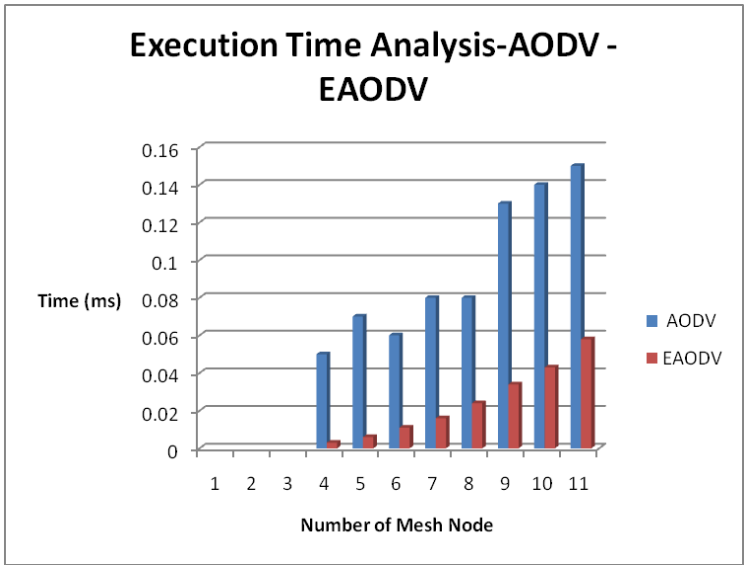

Fig 4.2 Execution Time Analysis- AODV-EAODV

V. CONCLUSION AND FUTURE WORKS

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 paper, 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.

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. The route discovery application if developed as web service, then many applications can make use of it. The new system becomes useful if the above enhancements are made in future. The new system is designed such that those enhancements can be integrated with current modules easily with less integration work.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 10, October 2017

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. 463-469,2007.
[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.
[14] J. Kulik, W. R. Heinzelman, and H. Balakrishnan, "Negotiation-based protocols for disseminating information in wireless sensor networks," Wireless Networks, Volume: 8, pp. 169-185, 2002.
[15] C. Schurgers and M.B. Srivastava, "Energy efficient routing in wireless sensor networks", in the MILCOM Proceedings on Communications for Network-Centric Operations: Creating the Information Force, McLean, V A, 2001.
[16] X. Huang, H. Zhai, Y. Fang, Robust cooperative routing protocol in mobile wireless sensor networks, IEEE Trans.WirelessCommun.7(12) (Dec. 2008) 5278–5285.
[17] G. S. Kumar, M. V. Vinu, P. G. Athithan, K. P. Jacob, Routing protocol enhancement for handling node mobility in wireless sensor networks, in: Proceedings of IEEE Region10Conference(TENCON), 2008,pp.1–6.
[18] D. Ganesan, B. Krishnamurthy, A.Woo, D. Culler, D. Estrin, and S. Wicker. "An empirical study of epidemic algorithms in large scale multihop wireless networks", Technical Report IntelIRP-TR-02-003, Intel Research, March 2002.
[19] D. Ganesan, R. Govindan, S. Shenker, and D. Estrin. "Highly resilient, energy efficient multi path routing in wireless sensor networks", MC2R, 1(2), 2002.
[20] Xiaoyan Hong, Mario Gerla, Guangyu Pei and Ching- Chuan Chiang. "A Group Mobility Model for Ad Hoc Wireless Networks", ACM International Workshop onModeling and Simulation of Wireless and Mobile Systems (MSWiM), August 1999.