Journal of Theoretical and Applied Information Technology
30th September 2014. Vol. 67 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

EFFECTIVE LIGHTWEIGHT TRUST DECISION MAKING SCHEME FOR WIRELESS SENSOR NETWORKS

[1]M.BALAMURUGAN, [2] Dr.R.POONGODI
[1]Research Scholar, Karpagam University, Coimbatore, India
[2]Department of ECE, PPG Institute of Technology, Coimbatore, India
E-mail: sabaalu@gmail.com

ABSTRACT

A sensor network is composed of a large number of sensor nodes, which are densely deployed either inside the phenomenon or very close to it. The position of sensor nodes need not be pre-determined. This allows random deployment in inaccessible terrains or disaster relief operations. On the other hand, this also means that sensor network protocols and algorithms must possess self-organizing capabilities. In this research work, a lightweight trust decision making scheme (LTDMS) for attaining balance between malicious nodes and energy conservation in networks. In first phase, multicast route is integrated to ensure network connectivity and avoid node failures. In second phase, key based authentication to provide integrity. Here four types of iterations are used during integrity phase. In third packet format is proposed for monitoring integrity and energy saving status. So the efficient secure multicast route can be chosen to improve the network performance. By simulation results, the proposed LTDMS achieves better data delivery rate, improved network lifetime, high packet integrity rate, less end to end delay and overhead in terms of mobility, pause time, throughput, and number of nodes than previous schemes namely HDTMP.

Keywords: *Wireless Sensor Networks, Malicious Nodes, Energy Saving, LTDMS, Packet Delivery Ratio, End to end delay, packet integrity rate and overhead.*

1. INTRODUCTION

The current technological advancement has already come to terms with immense potential of Wireless Sensor Network, Which consists of tiny sensor nodes scattered in a region communicating with each other over well defined protocols and transferring information of temperature, humidity etc between each other. Compared to ad hoc networks, sensor networks have some unique feature and application requirements.

Wireless sensor network generally composed of a large number of distributed sensor nodes that organize themselves into a multi-hop wireless network. Each network is equipped with more than one sensors, processing units, controlling units, transmitting units etc. Wireless sensor networks (WSN) are now used in many applications including military, environmental, healthcare applications, home automation and traffic control. It consists of a large number of sensor nodes, densely deployed over an area.

1.1 Security goals and threats of Wireless Sensor Networks WSNs

Based on the application, different architecture, goals and constraints have been considered for WSNs.

A. Eavesdropping

Eavesdropping occurs when an attacker compromises an aggregator node and listens to the traffic that goes through it without altering its behavior. Since aggregator nodes process various pieces of data from several nodes in the network, it does not only leak information about a specific compromised node, but from a group of nodes.

B. Data tampering and packet injection

A compromised node may alter packets that go through it. It may also inject false messages. Since an aggregate message embeds information from several sensor nodes, it is more interesting for an attacker to tamper with such messages than simple sensor readings. An attacker that controls the meaning of the malicious messages it sends may heavily impact the final result computed by the sink.

C. Denial of service (DoS)

A compromised node may stop aggregating and forwarding data. Doing so, it prevents the data sink from getting information from several nodes in the network. If the node still exchanges routing messages despite its unfair behavior, that problem may be difficult to solve. Smarter attacks also involve dropping messages randomly. It is also difficult to detect when an attacker sends garbage messages.

D. Ciphertext attack

It is an attack model for cryptanalysis in which the cryptanalyst gathers information, at least in part, by choosing a ciphertext and obtaining its decryption under an unknown key. In the attack, an adversary has a chance to enter one or more known ciphertexts into the system and obtain the resulting plaintexts. From these pieces of information the adversary can attempt to recover the hidden secret key used for decryption.

2. RELATED WORK

In this paper [1], it is investigated that how to secure route discovery of the Multicast Ad-hoc on Demand Distance Vector (MAODV) protocol for Sensor Networks. Compared to Ad hoc Networks, some secure routing protocols cannot be directly applied to energy constrained WSNs. In this research work, it was focused on secure route discovery of MAODV based on one way hash function. Here there is no signature generation proposed.

In this paper [2], authors presented an authentication scheme that uses public-key cryptographic scheme for authentication with an acceleration method for the signature verification in order to gain a high security level while preserving the limited resources in sensor networks. In this work, the distributed authentication model was proposed.

In this paper [3], a secure group communication scheme was proposed that allows sensor nodes belonging to the same group to communicate securely. It was composed of two main components: the group membership management and the group key management. First component defines in a secure manner the group creation, the group join and the group leave processes. The construction of a logical neighbor tree helps sharing the task of rekeying messages distribution among group members. This scheme eliminates the necessity of a powerful group controller and so that can fit resource-constrained sensor nodes.

In this paper [4],an efficient and secure geographical routing was presented against a series of attacks. This secure routing requires associative one-way hash function and security mechanism for security. It also makes use of the broadcast nature of wireless channel and forwards packets based on the opportunistic approach. Including this, one more routing metric is combined with this routing to defend against packet tempering and dropping incurred by the Sybil attack, wormhole attack, black hole attack, and so forth.

In this research work [5], it was given an overview of existing multicast protocols and investigate the performance of these protocols with respect to Qos metrics. The power multicast routing is also proposed and analysed with routing protocols.

In this paper [6], Bandwidth Efficient Cooperative Authentication scheme was proposed for filtering the injected false data, has been demonstrated to achieve not only high en-routing filtering probability but also high reliability with multi-reports. This scheme can be applied to distributed authentication purpose. It does not require a complex security fixation because it uses a non-interactive key establishment. In addition, it considers the situation that each node could be compromised, hence it distributes the en-routing authentication information to all sensor nodes on the routing path.

In this paper [7], it was presented an updated survey of genetic algorithm based multicast routing as a classification. Localization, mobility, query based, energy efficiency, data aggregation and QoS are the metrics used for the genetic algorithm based multicast routing in wireless sensor networks classification. Including this, a comparative study of all genetic algorithm based multicast routing techniques in wireless sensor networks was presented.

In this paper [8], it was introduced that a channel aware detection (CAD) algorithm that can effectively identify the selective forwarding misbehavior from the normal channel losses. The attack chosen here is Denial of Service attack. The algorithm is based on two strategies. With such an attack, a misbehaving mesh router just forwards a subset of packets it receives but drops the others. Both channel estimation and traffic monitoring was presented to estimate the normal loss rate due to bad channel quality or medium access collision and to monitor the actual loss rate.

The enhanced LEACH protocol [9] was proposed to protect networks against attacks such as, replay attacks, node compromising attacks and impersonation attacks. It performs better in terms of energy consumption, number of nodes alive, End-to-End Delay (EED), false data detection and aggregation accuracy.

In this paper [10], user authentication scheme was proposed based on elliptic curve cryptography for large scale hierarchical wireless sensor networks is presented. Elliptical provides mutual authentication between user and base station as well as base station and cluster head. It also provides option for dynamic node addition where there is no need to update any information in user smart card for accessing real time data for any addition or replacement of cluster heads in the networks.

In this paper [11], secure routing is vital to the acceptance and use of sensor networks for many applications, but we have demonstrated that currently proposed routing protocols for these networks are insecure. It was left that is an open problem to design a sensor network routing protocol that satisfies the proposed security goals.

The proposed scheme [12], advances the current state of the art by enabling not only the dynamic changing but the dynamic formation of multicast groups as well. A multicast encryption technique was proposed to achieve scheme efficiency and meet the resource constrained nature of WSNs.

In this paper [13], it was implemented a mutual authentication method based on the public key cryptography. After using this scheme, it is measured the performance of entire network using different parameters like Throughput, Load, Delivery ratio and energy consumption etc. For message authentication, during communication, encrypted message is sent by the nodes over network, and its hash is calculated, by sender and receiver decrypts the message and calculates the HASH again.

In this paper [14], Elliptical Curve Cryptography based user authentication protocol was proposed for WSNs. Thus, before issuing a query to a sensor node, each user must register with the gateway in a secure manner so that they can access the real-time sensors' data. Upon the successful user registration request, the gateway node personalizes a smart card for every registered user. Then, a user can submit his query in an authentic way and access the sensor network data at any time within an administratively configurable period.

In this paper [15], a hierarchical dynamic trust management protocol was proposed for cluster-based wireless sensor networks, considering two aspects of trustworthiness, namely, social trust and QoS trust. It was developed a probability model utilizing stochastic Petri nets techniques to analyze the protocol performance, and validated subjective trust against objective trust obtained based on ground truth node status.

In this research work [16], Optimal multiCast routing protocol (oCast) was proposed for sensor networks. It can effectively identify minimum energy multicast trees for small group multicast in intermittently connected sensor networks. In case the network is always connected, optimized multicast routing scheme can also construct optimal multicast trees. Furthermore, the multicast routing protocol does not rely on any specific unicast routing protocol, and it can provide the shortest end-to-end path from any sensor node to any sink by itself.

This paper [17], the secure broadcast was proposed in ad-hoc networks needs to jointly consider the physical and network layer algorithms to be energy-efficient. Developing efficient algorithms to allocate Key to members is the key distribution problem.

3. IMPLEMENTATION OF PROPOSED ALGORITHM

The proposed Effective Lightweight Trust Decision Making scheme consists of new multipath routing, integrated encryption/decryption scheme and energy consumption model to provide the authentication, integrity of the data and improve energy efficiency in sensor networks.

3.1 Multicast Routing Scheme

In Multicast Routing, the cluster head achieves the usual functions such as data replication, union and higher level transmission to the base station. At the onset, cluster heads are self-elected. It is allowed that the self-election for the first sets of cluster-heads. It is consistent with the initial assumption that there are no adversarial nodes at setup.

If the clusters are established, the cluster head schedules the transmission of each member in a Time Division Multiplexing and inform all the cluster members. If the current cluster head's battery power level falls below a predetermined threshold or serve for a predetermined period of time, it broadcasts a new election message within a cluster. All the mobile nodes then vote for a new cluster head by using secret vote. It is done by replying to the new election message with its choice of candidate. The reply, or vote, is encrypted with the pairwise key with the cluster head. Neighbor cluster members therefore have no idea of the political affiliation of each other since the key is private and, different for each node cluster head pair. The top pick from its list of trusted neighbors is selected as the node's candidate. The current cluster head then calculates the votes and decides the winner based on simple majority. The node with the second highest number of votes is chosen as the vice cluster head. The purpose of the junior cluster head is to assume cluster head function in the event that the newly elected cluster head fails before handing over to its successor. At the completion of calculating, the cluster head multicast the winner and runner-up to all the members of the cluster.

To achieve high integrity, the new winner and runner-up have to pass a challenge-response from the cluster head before they are allowed to take up office. If one or both of them fail the current cluster head informs the cluster members and, initiate a new election for the replacement of the corrupt nodes, which is defined here as the nodes that did not pass the challenge-response. The corrupt nodes are blacklisted in the cluster nodes' trust tables by setting its trust level value to -1. Once a node is set to -1 no further trust level update is done. Illustration of multicast route is shown in figure 1.

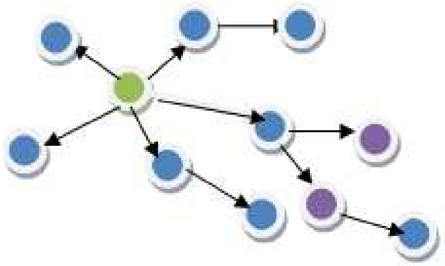

Figure1. Multicast Route Establishment

3.2 Multicast Route Establishment

Three modes are used.

On demand Mode :

In this mode, a node periodically sends out update packets to maintain the topology information.

Source Mode:

In this mode, a node will not periodically send out update packets and when receiving update packets from other nodes, it will just discard them.

On demand Ready Mode

In this mode, a node will not periodically send out update packets but updates its Neighbor Routing Table upon receiving the update packets from other nodes.

Path Finding Process

- If the node is in OM or ORM, the node first look in its Ntable to see whether there are nodes that belong to the destination multicast group. If so, the node unicasts Join Requests to all these nodes and waits for replies.
- When a node receives a Join Request, and it is a member of the multicast group, it generates the Reply and sends it back to the source of the Join Request, updating the Mtable to record the route.
- If the node could not send a Reply, it checks its own behavior. If it is in SM, it just propagate the Join Request and record the Join Request in the route cache.

3.3 Integrated Encryption/Decryption scheme

The digital signature scheme is a variant of the Optimized signature mechanism. Each entity creates a public key and corresponding private key. Each entity selects a finite group G; generator of G; public and private keys. Each entity A should do the following:

1. Generate a large random prime p and a generator α of the multiplicative group Z^*_p.
2. Select an appropriate cyclic group G of order n, with generator α. (Assume that G
is written multiplicatively.)
3. Select a random integer a, 1 ≤ a ≤ p − 2, Compute $y = \alpha^a$ mod p.
4. Select a random secret integer a, 1 ≤ a ≤ n−1. Compute the group element $y = \alpha^a$.
5. A's public key is (p,α, y), together with a description of how to multiply elements in G.

Entity signs a binary message m of arbitrary length. Any entity B can verify this signature by using A's public key.

Signature Generation:

1. Signature generation. Entity A should do the following:
(a) Select a random secret integer k, 1 ≤ k ≤ p − 2, with gcd (k, p − 1) = 1.
(b) Compute $r = \alpha^k$ mod p
(c) Compute k−1 mod (p − 1)
(d) Compute s = k−1{h(m) − a^r} mod (p − 1).
(e) A's signature for m is the pair (r, s).
(a) Compute the group element t = αq.
(c) Compute q−1 mod n.
(d) Compute h(m) and h(r).
(f) A's signature for m is the pair (r, s).

Signature Verification:

Verification. To verify A's signature (r, s) on m, B should do the following:
(a) Obtain A's authentic public key (p, α, y).
(b) Verify that 1 ≤ r ≤ p − 1; if not, then reject the signature.
(c) Compute v_1 = y mod p.
(d) Compute h(m) and v_2 = α h(m) mod p.
(e) Compute g_1 = yh(r) ▪ rs.
(d) Compute g_2 = αh(m).
(e) Accept the signature if and only if $v_1 = v_2$.
(g)Accept the signature if and only if $g_1 = g_2$.

4 *The proposed packet format*

The format of proposed packet format is shown in Fig. 1. The S_ID contains the node ID of source node. D_ID derives the node ID of the destination node.

S_ ID	D _ID	Hop Count	Seq. No.	Thres Energy	Integrity Status	Node Auth en.	C R C

Figure 2.Format Of The Proposed Route Request Message

The Hop Count field is the number of hops from the sink node which is used to identify nodes in different levels, nodes that can receive the radio signal of sink, threshold energy field provides the minimum required energy level for a node to be selected for data transmission. Integrity status field indicates that packet contains the data is genuine which is not altered or corrupted by any intruder. Node authenticity describes that destination node assures that the packet is sent from the authenticated source node. CRC means Cyclic Redundancy Check is used for error detection and correction.

4. PERFORMANCE ANALYSIS

We use Network Simulator (NS 2.34) to simulate our proposed LTDMS algorithm. Network Simulator-2(NS2.34) is used in this work for simulation.NS2 is one of the best simulation tools available for Wireless sensor Networks. We can easily implement the designed protocols either by using the oTCL (Tool command Language) coding or by writing the C++ Program. In either way, the tool helps to prove our theory analytically.

In our simulation, 200 mobile nodes move in a 1200 meter x 1200 meter square region for 60 seconds simulation time. All nodes have the same transmission range of 250 meters. Our simulation settings and parameters are summarized in table 2.

A. Performance Metrics

We evaluate mainly the performance according to the following metrics.

End-to-end delay: The end-to-end-delay is averaged over all surviving data packets from the sources to the destinations.

Packet Delivery Ratio: It is defined as the ratio of packet received with respect to the packet sent.

Throughput: It is defined as the number of packets received at a particular point of time

The simulation results are presented in the next part. We compare our proposed algorithm with our proposed LTDMS and HDTMP [15] in presence of energy consumption.

Table2. Simulation Settings And Parameters Of Proposed Algorithm.

No. of Nodes	200
Area Size	1100 X 1100
Mac	802.11
Radio Range	250m
Simulation Time	100 sec
Traffic Source	CBR
Packet Size	80 bytes
Mobility Model	Random Way Point
Protocol	LEACH

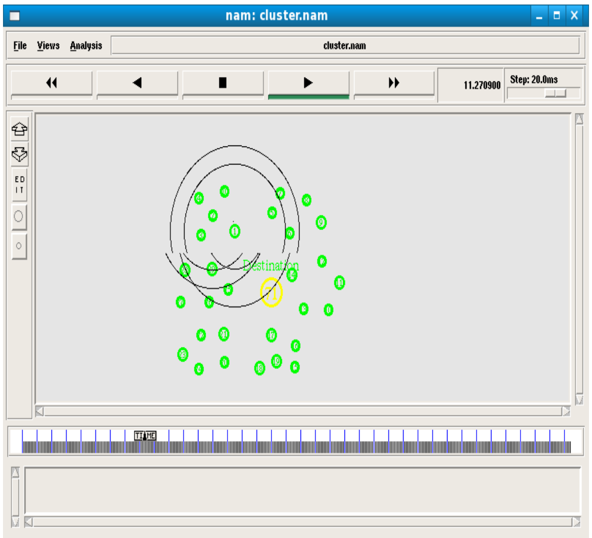

Figure 3. Topology Of The Proposed Scheme

Figure 3 shows that the proposed scheme topology for ensuring the multipath routing. Source node sends the packet to destination node via intermediate nodes. In case if the node failure occurs, the node choose the alternative path to reach correct delivery of packets.

Figure 4 presents the delivery ratio comparison for LTDMS, HDTMP, SBYaoGG. It is clearly seen that number of epochs consumed by LTDMS is high compared to HDTMP.

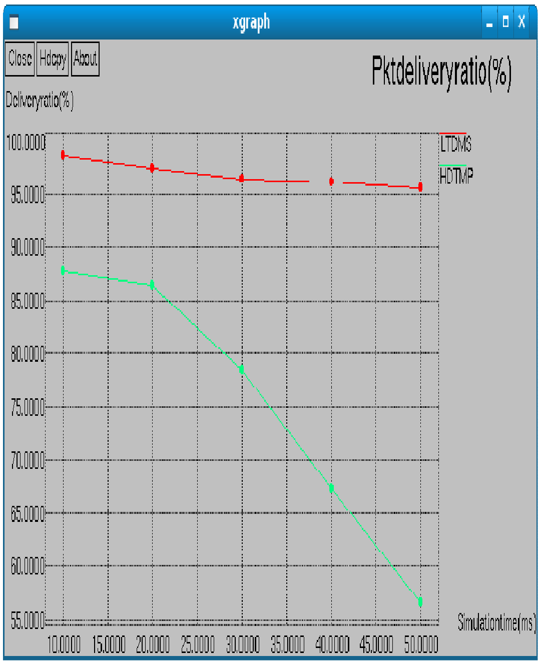

Figure 4. No.Of Nodes Vs Packet Delivery Ratio

Figure 5, presents the comparison of authentication rate. It is clearly shown that the authentication rate of LTDMS is higher than the HDTMP.

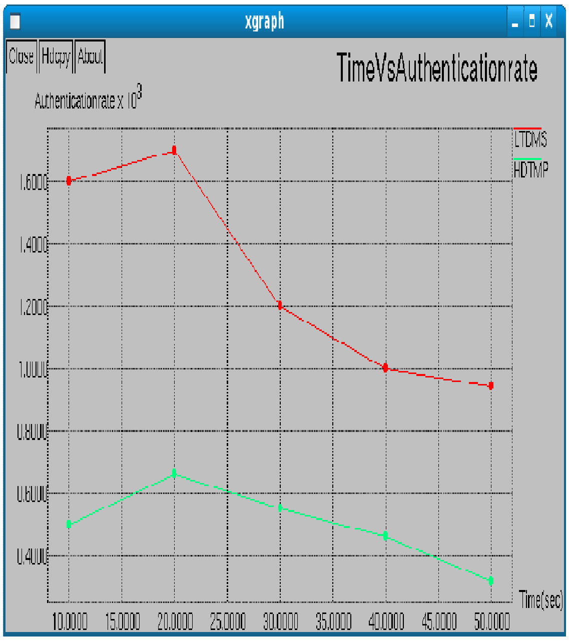

Figure 5. Time Vs Authentication Rate

Figure 6 shows the results of Mobility Vs End to end delay. From the results, we can see that LTDMS scheme has slightly lower delay than the HDTMP.

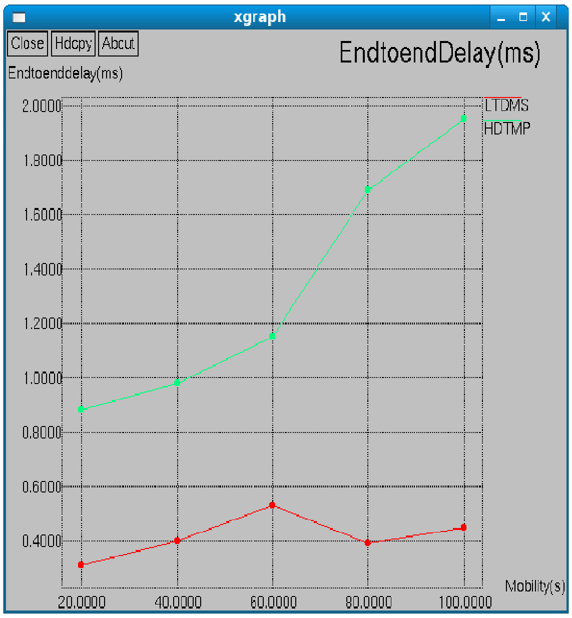

Figure 6. Mobility Vs End To End Delay

Figure 7, presents the comparison of overhead while varying the speed from 20 to 100 packets. It is clearly shown that the overhead of LTDMS is lower than the HDTMP.

.

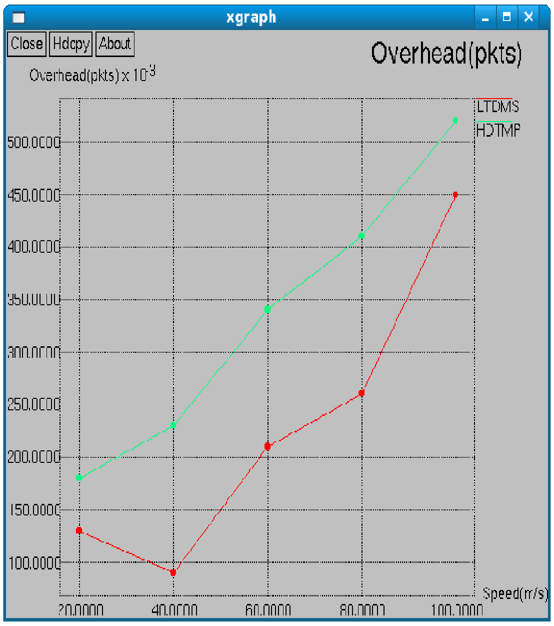

Figure 8. Mobility Vs Overhead

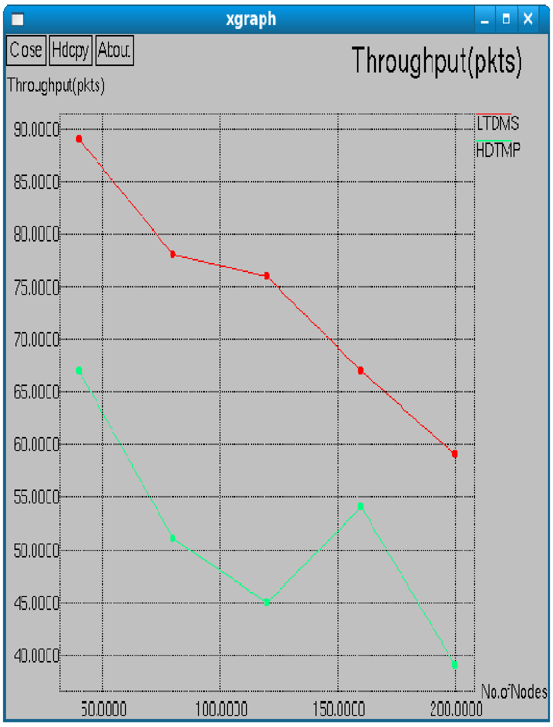

Figure 8. No. Of Nodes Vs Throughput

Figure 8 shows the results of throughput. From the results, we can see that scheme LTDMS has high throughput than HDTMP.

5. CONCLUSION

In WSNs, the best secure and energy efficient route is being determined by choosing efficient strategy to forward the data to the base station. Due to that, the node consumes more energy unnecessarily. Using clustering algorithms, nodes are grouped into clusters, and within each cluster, a node with strong computing power is elected as a cluster head (CH). CHs together form a higher-level backbone network. In the proposed scheme, multicast routing is enhanced with LTDMS which attains the problem of malicious nodes and link breakage. The proposed scheme LTDMS achieves better performance than existing schemes. In future, we have planned to implement elliptical curve cryptography technique to make network more secure. By simulation results we have shown that the LTDMS achieves increased delivery ratio, low end to end delay, low overhead, good throughput, high authentication rate while attaining low delay than existing scheme HDTMP while varying the number of nodes, time, node throughput and mobility.

REFERENCES

[1] .Shyamala and Dr.S.Valli, “Securing Route Discovery in MAODV for Wireless Sensor Networks”, *Ubiquitous Computing and Communication Journal,* Vol.4, No.3, 2009, pp.775-783.

[2] Nourah Al-Angari and Mznah Al-Rodhaan, “ Accelerating Signature-Based Broadcast Authentication In Decentralized Wireless Sensor Networks”, *Journal of Theoretical and Applied Information Technology*, Vol.52, No.3, 2013, pp.366-369.

[3] Omar Cheikhrouhou,, Anis Koubâa, Gianluca Dini, Hani Alzaid, Mohamed Abid, “LNT: A Logical Neighbor Tree Secure Group Communication Scheme for Wireless Sensor Networks”, *Elsevier,* Procedia Computer Science, 2012, pp.1-47

[4] Chen Lyu, Dawu Gu, Yuanyuan Zhang, Tingting Lin, and Xiaomei Zhang, “Towards Efficient and Secure Geographic Routing Protocol for Hostile Wireless Sensor Networks”, *International Journal of Distributed Sensor Networks,* 2013, pp.1-11.

[5] M. A. Khan, M. Ahsan, G. A. Shah, Muhammad Sher, “Multicast Routing Protocols in Wireless Sensor Networks”, *Journal of Computing*, Vol. 4, Issue 9, September 2012,pp.9-17.

[6] Nithya Menon, S.Praveena, “ BECAN: A Bandwidth Efficient Cooperative Authentication Scheme for Wireless Sensor Networks”, *International Journal of Innovative Technology and Exploring Engineering*, Vol.2, Issue 6, 2013, pp.112-115.

[7] J.Suresh Kumar, E.Babu Raj, “ Genetic Algorithm based Multicast Routing in Wireless Sensor Networks - A Research Framework”, *International Journal of Engineering and Innovative Technology*, Volume 2, Issue 6, 2012, pp.240-246.

[8] Anand Nayyar, “ Trust Based Selective Forwarding Attacks using Channel Aware Approach in Wireless Mesh Networks”, *Journal of Information and Computing Science*, Vol. 7, No. 4, 2012, *pp*. 296-302.

[9] A. Gopi Saminathan and S. Karthik, “Development of an Energy efficient, Secure and Reliable Wireless Sensor Networks Routing Protocol Based on Data Aggregation and user Authentication”, *American Journal of Applied Sciences*, Vol.10, No.8, 2013, pp.832-843.

[10] Rakesh Maharana and Pabitra Mohan Khilar, " An Improved Authentication Protocol for Hierarchical Wireless Sensor Networks using ECC", *International Journal of Computer Applications*, Vol.67, No.22, 2013, pp.23-30.

[11] Chris Karlof and David Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", *DARPA Funding*, pp.1-15.

[12] Kui Ren, Wenjing Lou, Bo Zhu and and Sushil Jajodia, "Secure and Efficient Multicast in Wireless Sensor Networks Allowing Ad hoc Group Formation", *IEEE Transactions on Vehicular Technology*, Vol. 58, No. 4, 2009, pp.2018-2029.

[13] Shweta Goel , Manjeet Behniwal and Ajay Kumar Sharma, " Authentication and Key Distribution Schemes for Wireless Sensors Network", *International Journal of Advanced Research in Computer Science and Software Engineering*, Vol.3, Issue 7, 2013, pp.1343-1350.

[14] Wenbo Shi and Peng Gong, "A New User Authentication Protocol for Wireless Sensor Networks Using Elliptic Curves Cryptography", *International Journal of Distributed Sensor Networks*, 2013, pp.1-18.

[15] Fenye Bao, Ing-Ray Chen, MoonJeong Chang, and Jin-Hee Cho, "Hierarchical Trust Management for Wireless Sensor Networks and its Applications to Trust-Based Routing and Intrusion Detection", *IEEE Transactions on Network and Service Management*, Vol. 9, No. 2, 2012, pp.169-183.

[16] Lu Su, Bolin Ding, Yong Yang, Tarek F. Abdelzaher, Guohong Cao and Jennifer C. Hou, "Optimal Multicast Routing Protocol for Wireless Sensor Networks", *National Science Foundation,* pp.1-10.

[17] Loukas Lazos, Radha Poovendran, " Secure Broadcast in Energy-Aware Wireless Sensor Networks", *ARO grant*, pp.1-2.