Journal of Theoretical and Applied Information Technology
10th January 2014. Vol. 59 No.1

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

SECURE AUTHENTICATION BASED MULTIPATH ROUTING PROTOCOL FOR WSNS

[1]N.SUMA, [2] DR.T.PURUSOTHAMAN

[1] Research Scholar, Anna University, Chennai, India
[2] Associate Professor, Department of Computer Science and Engineering ,
Government College of Technology, Coimbatore, India.
E-mail: kalai_suma@yahoo.com

ABSTRACT

Wireless sensor networks consist of some nodes that have limited processing capability, small memory and low energy source. These nodes are deployed randomly and often densely in the environment. In order to avoid malicious activities, the secure authentication scheme is required. Here, we have proposed the Secure Authentication based Multipath Routing Protocol (SAMRP) for improving network lifetime and providing data integrity in WSNs. It consists of three phases. In first phase, multipath route is integrated to ensure load balancing and avoid isolated failures. In second phase, encryption and decryption scheme is implemented to provide better authentication. Here three types of iterations are used during authentication phase. In third packet format is proposed for monitoring integrity and authentication status. So the efficient secure multipath route can be chosen to improve the network performance. By simulation results, the proposed SAMRP 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 the our previous scheme EMRTEM and existing scheme ADAPT.

Keywords: *WSN, SAMRP, Encryption And Decryption, Multipath Routing, Packet Integrity Rate, Network Lifetime, End To End Delay, Communication Overhead, Throughput And Data Delivery Rate.*

1. INTRODUCTION

Wireless sensor networks (WSN's) have attracted a great deal of research attention due to their wide-range of potential applications. Applications of WSN include battlefield surveillance, biological detection, medical monitoring, home security and inventory tracking. This type of network consists of a group of nodes and each node has limited battery power. There may be many possible routes available between two nodes over which data can flow. Assume that each node generated some information and this information needs to be delivered to a destination node. Any node in the network can easily transmit their data packet to a distance node, if it has enough battery power. If any node is far from its neighbour node then large amount of transmission energy is required to transmit the data to distance node. After every transmission, remaining energy of this node decreases and some a counts of data transmission this node will be eliminated from the network because of empty battery power and in similar situation there will be a condition that no node is available for data transmission and overall lifetime of network will decreases.

B. Design goals of Wireless Sensor Networks WSNs)

Based on the application, different architecture, goals and constraints have been considered for WSNs. The design goals are given below.

- **Unattended operation** – Sensor networks can be deployed in unattended environments, therefore there is a risk of physical attacks on the sensor nodes. Also, the sink might not be present at all times. The sensor network has to continue its operation in the presence of compromised and/or destroyed nodes and when the sink is not present.
- **Resource limitation** – The nodes have limited memory which has to be considered both when collecting data and when developing software and security solutions, e.g., keying material might require a lot of storage for a long period of time.
- **Computational power** – Sensors usually have limited computational power which limits the choice of security mechanisms.
- **Power consumption** – As sensor nodes are battery driven, all applications running on nodes should try to limit their energy consumption as much as possible. One of the most energy consuming tasks is transmitting

and receiving messages. The protocols/applications used should not only minimize the power consumption of individual nodes, it should also try to minimize the power consumption in the entire network. Many security protocols, especially the ones using public key cryptography, require long messages, and has therefore high power consumption.

- **Wireless medium** – All communication in a sensor network is wireless. The wireless medium is prone to interference, resulting in unreliable communication, and it is also easy to eavesdrop on. The eavesdropping is further made easy by the fact that a sensor network is usually deployed in an unattended environment. It is also quite easy to insert messages on the wireless channel.
- **Reliability** – Due to the nature of the cheap hardware, node failure is a concern. Redundancy is a good solution for dealing with cheap and unreliable hardware. A security protocol should therefore not count on all nodes being able to reply at all times and be able to use the redundancy in the system.
- **Multi-hop communications** – The risk for messages to be modified or dropped increases with the number of hops the message must travel.

.

C. Security goals and threats

Ideally, one would like the network security to degrade gracefully with the number of compromised nodes. We consider three types of attack and assume that some link-level security mechanism is implemented to protect the network against these attacks in the absence of node compromise.

- **Eavesdropping:** Eavesdropping occurs when an attacker compromises an aggregator node and listens to the traffic that goes through it without altering its behavior. Since an aggregator node processes 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.
- ***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.
- **Denial of Service:** 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.

2. RELATED WORK

Jing Deng et.al [1] focused on the design of a secure and INtrusion-tolerant routing protocol for wireless Sensor NetworkS (INSENS). INSENS constructs secure and efficient tree-structured routing for WSNs, and is tailored for the asymmetric architecture and resource constraints of WSNs. A key objective of INSENS is to localize the damage caused by an intruder who has compromised deployed sensor nodes. Such an intruder could inject, modify, or block data packets, and in the worst case could bring down the entire sensor network, e.g. by flooding malicious packets. INSENS is therefore designed to tolerate intrusions, limiting the ability of an intruder to cause mischief through a combination of distributed lightweight security mechanisms.

Sasikala V and C. Chandrasekar [2] developed a technique which combines energy efficiency and multiple path selection for data fusion in WSN. The network is partitioned into various clusters and the node with highest residual energy is selected as the cluster head. The sink computes multiple paths to each cluster head for data transmission. The distributed source coding and the lifting scheme wavelet transform are used for compressing the data at the cluster head. During each round of transmission, the path is changed in a round robin manner, to conserve the energy. This process is repeated for each cluster.

Yang Yuwang et.al [3] proposed a Reliable Braided Multipath Routing with Network Coding for underwater sensor networks (RBMRNC) . Disjoint multipath algorithm is used to build independent actual paths, as called main paths. Some braided paths on each main path are built according to the braided multipath algorithm, which are called logic paths. When a data packet is transmitted by these nodes, the nodes can employ network coding to encode packets coming from the same group in order to further reduce relativity among these packets, and enhance the probability of successful decoding at the sink node. Braided multipath can make the main paths to be multiplexed to reduce the probability of long paths.

Mary Cherian and Gopalakrishnan nair [4] proposed a multipath routing algorithm which enables the reliable delivery of data. By controlling the scheduling rate, it is possible to prevent congestion and packet loss in the network. The algorithm provides an efficient way to prevent the packet loss at each node. This results in congestion management in the sensor networks. This protocol prevents packet clustering and provides smoothness to the traffic. Through monitoring and controlling the scheduling rate the flow control and congestion control are managed.

S. Saqaeeyan and M. Roshanzadeh [5] presented the reliable and energy aware packet delivery mechanism to ensure quality of service in wireless sensor networks. In the proposed algorithm to ensure that a packet of information sent to the destination, the multi-path forwarding method is used; So that several copies of an information packet via separate routes are sent to the destination, also routing decisions in this way occurs by considering the remaining energy in the neighborhood of nodes that are located in two hop of sender node.

Senthil kumar et.al [6] analyzed the base station which is used to provide individual base station attacks or sensor node compromises problem to design a sensor network routing protocol that satisfies the proposed security goals. One aspect of sensor networks organized hierarchically, with a base station serving as a gateway for collecting data from a multi-hop network of resource-constrained sensor nodes.

Hamid reza Hassaniasl et.al [7] proposed score aware routing algorithm which consists of five parameters namely closeness to sink node, node remaining energy, sent traffic by node in the previous phase, number of successful and fault-free sent packets, and the number of observed sources in one node for scoring to the node during routing process. The nodes with higher score have higher chance for selection as path middle nodes. The main objectives of this method are; decrease of consumption energy and the uniform distribution, increase of network lifetime, decrease of traffic load and load balance, possibility of more effective aggregation of data and improving the reliability of formed paths.

Venkata Sumanth Mareedu et.al [8] explored how broadcast how broadcast trustworthiness interacts by flooding in wireless networks. Whereas there is an immense deal of prior work in the area of reliable broadcast, the majority of it focuses on efficient flooding, in simulated topologies, frequently with multi-hop topological information. We instead focused on the end-to-end reliability of flooding and the study of topologies with erratic density as we originate in our testbed. In addition, it is proposed a very straightforward mechanism that uses only local density information, sometimes augmented by ndications from instant neighbors of significant relations.

Saleem et.al [9] proposed an enhanced ant colony inspired self-organized routing mechanism for WSNs. The specified mechanism is based on delay, energy and velocity. The adopted factors and reinforcement learning (RL) feature help WSN in improving the overall data throughput; especially in case of real time traffic. The algorithm is also capable to avoid permanent loops which promotes dead lock problem in the running networks. The dead lock problem is cured by assigning unique sequence ID to every forward ANT and also to search ANT. Simulation results clearly demonstrate the protocol efficiency and also verify that the protocol is practicable. Furthermore, this algorithm is enhanced with the multipath feature to reduce congestion situations in WSN. Finally, this autonomic routing mechanism will come up with better data throughput rate while minimizing packet loss.

Song Han et.al [10] explored novel coding-aware multi-path routing protocol (CAMP), which forwards packets over multiple paths dynamically based on path reliability and coding opportunity. CAMP employs a route discovery mechanism which returns to the source multiple paths along with ETX (Expected Transmission Count) of all links on each path. Using a novel forwarding mechanism, CAMP splits the traffic among multiple paths and actively creates instead of passively waiting for coding opportunity by switching its path to maximize the switching gain.

Tanveer A. Zia and Albert Y. Zomaya [11] presented a computationally lightweight security framework to provide a comprehensive security solution against the known attacks in sensor networks. The proposed framework consists of four interacting components: a secure triple-key scheme (STKS), secure routing algorithms (SRAs), a secure localization technique (SLT) and a malicious node detection mechanism. Singly, each of these components can achieve certain level of security. However, when deployed as a framework, a high degree of security is achievable. The framework takes into consideration the communication and computation limitations of sensor networks. Once the network is deployed, base station builds a table containing unique identity of all the nodes in the network. After self organizing process base station knows the topology of the network. Nodes use our secure triple-key management scheme to collect the data, pass onto the cluster leader which aggregates the data and sends it to the base station.

Wenjing Lou [12] proposed a distributed N-to-1 multipath discovery protocol, based on a hybrid multipath scheme to achieve both more reliable and more secure data collection task in wireless sensor networks. While most of multipath routing protocols are source-initiated and aim to find multiple disjoint or partially disjoint paths between a single source-destination pair, the distinct feature of N-to-1 multipath discovery protocol is that it is receiver-initiated (i.e., BS initiated) and at the end of one route discovery process, the protocol finds every sensor node a set of node-disjoint paths to the BS simultaneously. It is highly efficient, with an average overhead of less than one routing message per path. A hybrid multipath data collection scheme is developed which combines end-to-end multipath data dispersion and per-hop alternate path routing to improve both reliability and security.

Ravindra Gupta and Hema Dhadhal [13] explored general security threats in wireless sensor network and made an extensive study to categorize available data gathering protocols and analyze possible security threats on them. Due to limitations of sensor devices, the networks exposed to various kinds of attacks and conventional defenses against these attacks are not suitable due to the resource constrained nature of these kinds of networks. Secure routing protocols in wireless sensor network were represented focusing on the problem and the methodology in order to solve the problem.

Suraj Kumar Sharma & Sanjay Kumar Jena [14] proposed a secure cluster based multipath routing protocol (SCMRP). The SCMRP is the combination of these two sensor networks; therefore, it provides efficiency as well as reliability and the proper use of cryptographic algorithm provides sufficient security to the sensor network. SCMRP provides security against various attacks like altering the routing information, selective forwarding attack, sinkhole attack, wormhole attack, Sybil attack etc. SCMRP mainly consists of five phase; neighbor detection and topology construction, pairwise key distribution, cluster formation, data transmission and re-clustering and re-routing.

Xiaoxia Huang and Yuguang Fang [15] introduced QoS multipath routing to provide soft QoS to different packets as path information is not readily available in wireless networks. The multiple paths are utilized between the source and sink pairs for QoS provisioning. Unlike E2E QoS schemes, soft-QoS mapped into links on a path is provided based on local link state information. By the estimation and approximation of path quality, traditional NP-complete QoS problem can be transformed to a modest problem. The idea is to formulate the optimization problem as a probabilistic programming, then based on some approximation technique, we convert it into a deterministic linear programming, which is much easier and convenient to solve. More importantly, the resulting solution is also one to the original probabilistic programming.

Tao Shu et.al [16] proposed randomized multi-path routing algorithm which can be applied to to selective packets in WSNs to provide additional security levels against adversaries attempting to acquire these packets. By adjusting the random propagation and secret-sharing parameters (*N* and *M*), different security levels can be provided by our algorithms at different energy costs. Considering that the percentage of packets in a WSN that require a high security level is small, it is believed that the selective use of the proposed algorithms does not significantly impact the energy efficiency of the entire system. The proposed work is based on the assumption that there is only a small number of black holes in the WSN. In reality, a stronger attack could be formed, whereby the adversary selectively compromises a large number of sensors that are several hops away from the sink to form clusters of black holes around the sink. Collaborating with each other, these black holes can form a cut around the sink and can block every path between the source and the sink.

Wenjing Lou and Yuguang Fang [17] proposed a novel approach to enhance data confidentiality service in the network. The idea is to integrate the secret sharing scheme and multipath routing. The secret sharing scheme is described that how it is applied to the secure message to be transmitted. After that the distributed multipath routing algorithm is developed to find the desired multiple paths. The algorithm takes path independence, path quantity, as well as path cost into consideration. The simulation is shown that with comparably low complexity, the proposed algorithm is able to find, for each source destination pair in the network, a set of disjoint paths.

Hannes Frey et.al [18] proposed new multicast generalization with fast recovery mechanism to achieve a delivery of multicast message, to improve energy efficiency and path to the destination messages. The proposed solution is based on minimum spanning tree (MST) which requires information only on single hop neighbors. A message replication occurs when the MST spanning the current node and the set of destinations has multiple edges originated at the current node. Destinations spanned by these edges are grouped together, and for each of these subsets the best neighbor is selected as the next hop. This selection is based on a cost over progress metric, where the progress is approximated by subtracting the weight of the MST over a given neighbor and the subset of destinations to the weight of the MST over the current node and the subset of destinations.

The paper is organized as follows. The Section 1 describes introduction about WSNs, design goals, security goals and threats of WSNs. Section 2 deals with the previous work which is related to the multipath routing and secure authentication models. Section 3 is devoted for the implementation of proposed scheme. Section 4 describes the performance analysis and the last section concludes the work.

3. IMPLEMENTATION OF PROPOSED SCHEME

In the proposed scheme, multipath route is deployed to improve the load balancing and network lifetime. The encryption and decryption scheme is proposed to provide both authentication and data integrity against the malicious activities. So each node can assure authenticated route as well as node. The following describes the proposed multipath and secure authentication scheme. The flow of SAMRP is illustrated in figure 1.

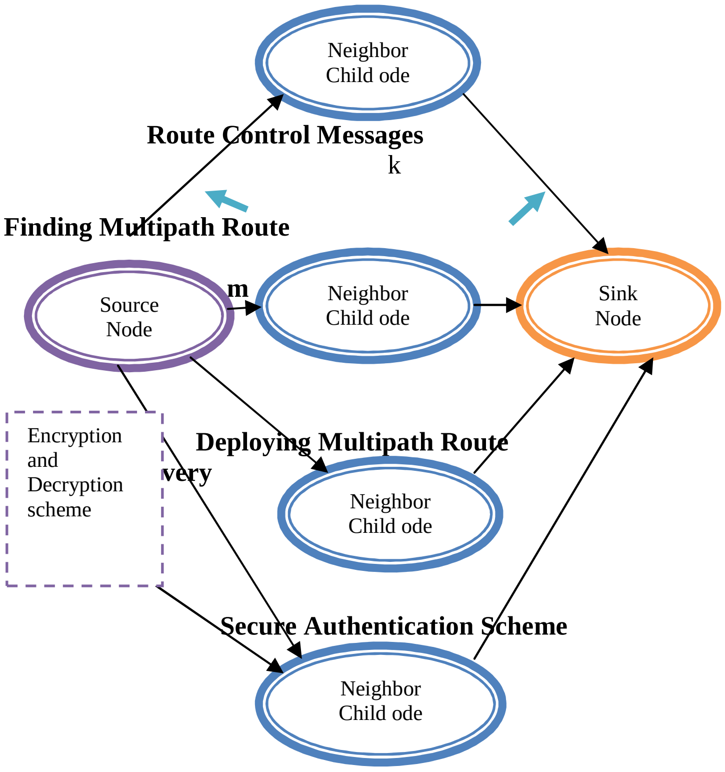

Figure 1. Process Flow Of Proposed Approach

3.1 Multipath Routing Scheme

Node supports with number of mobile nodes in its neighbourhood without relying on a single node to forward a message. If any failure of message arrival, it can be sent on alternative path or on multipath in parallel. So the impact of isolated failures is reduced. In the proposed scheme, multipath routing has been used mostly for fault tolerance and load balancing, and for failure recovery. The communication between mobile node and its neighbor node happens either through a direct communication path or through at most one neighbor. This guarantees that on any communication path between two nodes, there exist two disjoint authentication paths. The following procedure is for message forwarding in multipath routing. Consider a message travelling a path A_0; $A_{1,}$ A2…….A_k is authenticated twice before it is forwarded. A_0 creates Message Authentication Code (MAC) intended for nodes A_1 and A_2. A_0 can only reach A_1 directly and relies on S1 to transmit the MAC intended for S2. Before S1 forwards the message, it creates two new authentication codes itself for A_2 and A_3. It is continued until the message reaches its final destination. Before a node forwards a message, it checks the authentication codes from the two preceding nodes. If both codes indicate that the message has not been manipulated, the node forwards the message. An exception arises when a message is created, where only one MAC needs to be checked by the immediate neighbour of the source node. It is obvious that two adjacent nodes can cooperatively compromise the communication path. It is able to manipulate and inject arbitrary messages that are routed through them. This seems to be only a slight improvement over simple hop-to-hop authentication at first. Instead of compromising one node, an attacker now has to gain control over two of them. And since they are co-located, an attack should be easy. Thus it seems nothing much is gained. The following figure shows the representation of multipath routing.

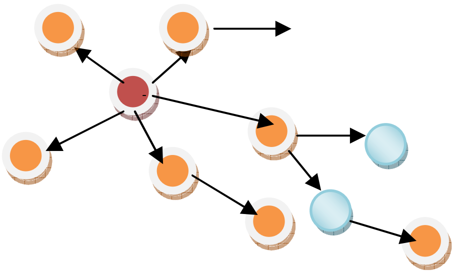

Figure 2. Multipath Routing Approach

Procedure for Route discovery process in Multipath Routing

```
S wants to establish a connection with D
Initialize START list
Initialize STOP list
Set start node as node_start
Set stop node as node_stop
for each node K between node_start to node_stop
Estimate Delay and authentication status  for each
    node
Calculate energy level and data integrity of each
    node
Store all values in routing table of each node
end for
Add node_start to the START list
while the START list is not empty
Get node n off the START list with the lowest l(n)
Add n to the STOP list
if n is the same as node_stop it is found the
    solution;
return Solution(n)
Generate each descendant node n' of n
for each descendant node n' of n
Set the parent of n' to n
Set h(n') to be the heuristically estimate
Delay and authentication status to node_stop
Set g(n') to be g(n) plus the packet loss rate and
    data integrity to get to n' from n
Set f(n') to be g(n') plus h(n')
if n' is on the START list and the existing one is
    as
    good or better
then
discard n' and continue
if n' is on the STOP list and the existing one
is as good or better then
discard n' and continue
Remove occurrences of n' from START and
    STOP
Add n' to the START list
return failure
```

A. *Secure Authentication Scheme*

In this phase, both encryption and decryption schemes are implemented. Here three types of iterations are used while converting plaintext to ciphertext. In first iteration, plaintext is converted into ASCII value. In second, ASCII is converted into BCD value. In third, BCD is converted in to Hexadecimal value.

The following cryptographic primitives are used in PSEC:

1. KDF is a key derivation function that is constructed from a hash function.

2. ENC is the encryption function for a symmetric-key encryption scheme such as the AES, and DEC is the decryption function.

3. MAC is a message authentication code algorithm such as HMAC.

Encryption phase

INPUT: Domain parameters $D = (q,FR, S,p,q, P,n,h)$, public key Q, plaintext m.
OUTPUT: Ciphertext (R,C, s, t).
1. Select $r \in R$ $\{0,1\}l$, where l is the bitlength of n.
2. $(k', k1, k2) \leftarrow$ KDF(r), where k' has bitlength l +128.
3. Compute $k = k'$ mod n.
4. Compute $R = kP$ and $Z = kQ$.
5. Compute $s = r \in$ KDF(R, Z).
6. Compute $C =$ ENC$k1(m)$ and $t =$ MAC$k2\ (C)$.
7. Return(R,C, s, t).

Decryption phase

INPUT: Domain parameters $D = (q,FR, S,p,q, P,n,h)$, private key d, ciphertext (R,C, s, t).
OUTPUT: Plaintext m or rejection of the ciphertext.
1. Compute $Z = dR$.
2. Compute $r = s\in$ KDF(R, Z).
3. $(k\_ , k1, k2) \leftarrow$ KDF(r), where $k\_$ has bitlength l +128.
4. Compute $k = k'$ mod n.
5. Compute $R' = kP$.
6. If $R' \;\; = R$ then return(“Reject the ciphertext”).

7. Compute *t'* = MAC*k*2*(C)*. If *t* = *t* then return("Reject the ciphertext").
8. Compute *m* = DEC*k*1*(C)*.
9. Return(*m*).

Proof for Decryption: If ciphertext *(R,C, s, t)* was indeed generated by the legitimate entity when encrypting *m*, then *dR = d(kP) = k(dP) = kQ*. Thus the decryptor computes the same keys *(k', k*1*, k*2*)* as the encryptor, accepts the ciphertext, and recovers *m*.

B. Proposed packet format

Source ID	Destination ID	Authentication Status	Packet Integrity Status	Energy Conservation Rate	CRC
2	2	4	4	4	2

Figure 3.Proposed Packet Format

In figure 3. the proposed packet format is shown. Here the source and destination node ID carries 2 bytes. Third one is authentication status of the node. The authentication status induces the whether the transmission of packets are travelled through authenticated route. In fourth field, the packet integrity status is indicated. It determines how much of the genuine packets are transmitted between source and destination node. It also determines whether packet contains authorized information. In fifth, the energy conservation ratio is allotted to ensure minimum energy consumption. The last filed CRC i.e. Cyclic Redundancy Check which is for error correction and detection in packet while route maintenance process.

4. PERFORMANCE ANALYSIS

We use Network Simulator (NS2.34) to simulate our proposed algorithm. Network Simulator-3 (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 coding or by writing the C++ Program. In either way, the tool helps to prove our theory analytically. In our simulation, 250 mobile nodes move in a 1600 meter x 1600 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 1.

Table 1. Simulation Settings And Parameters Of SAMRP

No. of Nodes	250
Area Size	1600 X 1600
Mac	802.11
Radio Range	250m
Simulation Time	60 sec
Traffic Source	CBR
Packet Size	512 bytes
Mobility Model	Random Way Point
Transmitter Amplifier	150 pJ/bit/m^2
Package rate	5 pkt/s
Protocol	LEACH

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 the ratio of packet received to packet sent successfully. This metric indicates both the loss ratio of the routing protocol and the effort required to receive data. In the ideal scenario the ratio should be equal to 1.

Communication Overhead: It is defined as the total number of routing control packets normalized by the total number of received data packets.

Throughput: It is defined as the number of packets received successfully.

The simulation results are presented in the next part. We compare our proposed scheme SAMRP with EMRTEM, ADAPT in presence of secure authentication.

Figure 4 shows the results of packet integrity rate for varying the speed from 20 to 100 msec. From the results, we can see that SAMRP scheme has more packet integrity rate than the EMRTEM and ADAPT schemes.

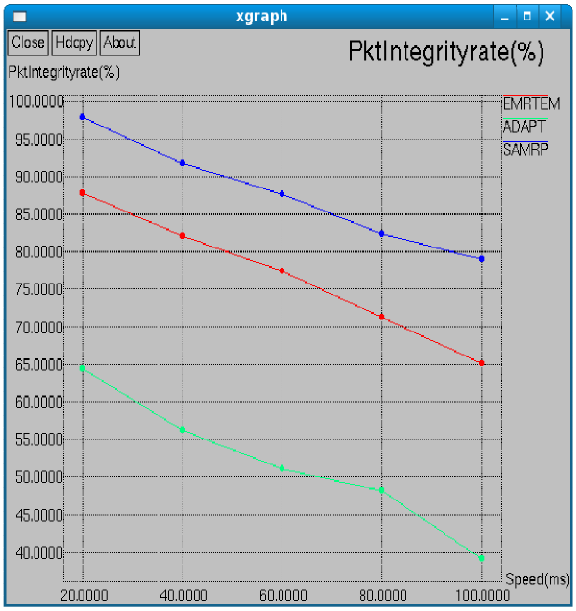

Figure 4. Speed Vs Packet Integrity Rate

Figure 5 shows the results of communication overhead for varying the mobility from 20 to 100. From the results, we can see that SAMRP has communication overhead than the EMRTEM and ADAPT schemes.

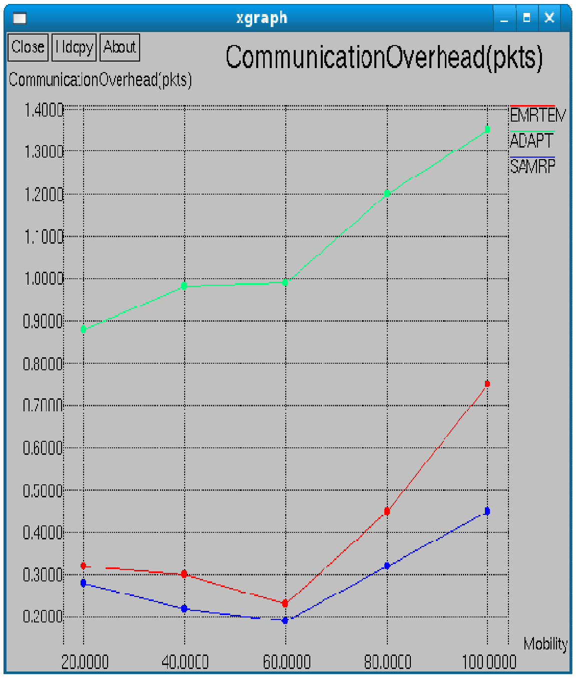

Figure 5. Mobility Vs Communication Overhead

Figure 6 presents the network lifetime comparison for SAMRP, EMRTEM, ADAPT. It is clearly seen that number of epochs consumed by SAMRP is high compared to ADAPT and EMRTEM.

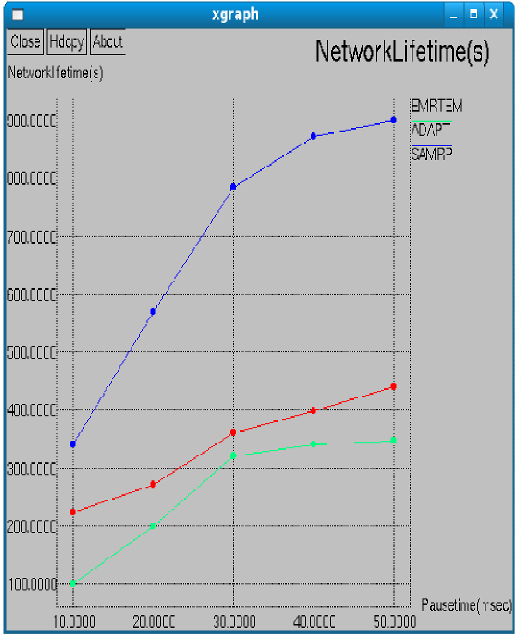

Figure 6. Pausetime Vs Network Lifetime

Figure 7 presents the comparison of data delivery rate. It is clearly shown that the data delivery rate of SAMRP is higher than the EMRTEM and ADAPTS schemes.

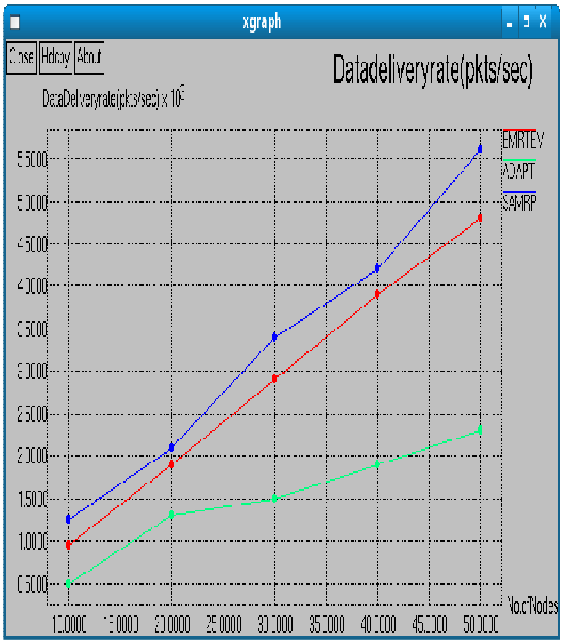

Figure 7. No. Of Nodes Vs Data Delivery Rate

Figure 8 shows the results of Time Vs End to end delay. From the results, we can see that SAMRP scheme has slightly lower delay than the EMRTEM and ADAPT scheme because of secure authentication routes.

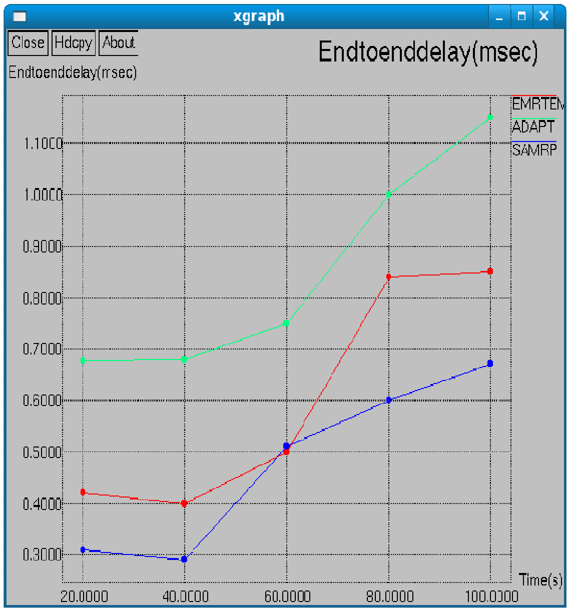

Figure 8. Time Vs End To End Delay

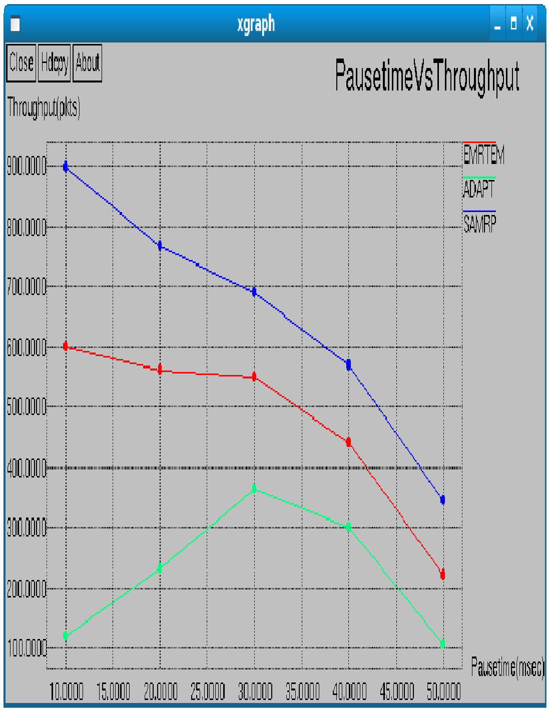

Figure 9 Pause Time Vs Throughput

Figure 9 presents the comparison of throughput. It is clearly shown that the throughput of SAMRP is higher than the EMRTEM and ADAPTS schemes.

5. CONCLUSION

In this research work, we have developed a Secure Authentication based Multipath Routing Protocol which attains Establishment of Multipath Routing and Authentication scheme to make a correct balance between network life time, data integrity and throughput to the sensor nodes. In the first phase of the scheme, multipath routing is proposed. In second phase, secure authentication scheme is deployed to protect data against malicious activities. In third phase, packet format is proposed. It contains following factors packet integrity status, authentication status to favour better route selection and reduce the effect of malicious activities by maintaining high secure authentication for each node. We have demonstrated the multipath route discovery procedure of each node. By simulation results we have shown that the SAMRP achieves good throughput, high network lifetime, high packet integrity rate, good data delivery rate while attaining low end to end delay, low overhead than the existing schemes EMRTEM, ADAPT while varying the number of nodes, speed, mobility and pause time.

REFERENCES:

[1] Jing Deng, Richard Han, Shivakant Mishra, “INSENS: Intrusion-tolerant routing for wireless sensor networks”, *Computer Communications, Elsevier*,2005, pp. 1–15.

[2] Sasikala V and C. Chandrasekar, “Energy Efficient Multipath Data Fusion Technique for Wireless Sensor Networks”, *ACEEE Int. J. on Network Security* , Vol. 03, No. 02, April 2012, pp.34-41.

[3] YANG Yuwang, JU Yutao, ZHENG Ya, SUN Yamin and YANG Jingyu, “Reliable Braided Multipath Routing with Network Coding for Underwater Sensor Networks”, *China Ocean Engineering* , Vol. 24, No. 3, 2010 pp. 565- 574.

[4] Mary Cherian& T. R. Gopalakrishnan Nair, “Multipath Routing With Novel Packet Scheduling Approach In Wireless Sensor Networks”, *International Journal of Computer Theory and Engineering*, Vol. 3, No. 5, 2011, pp.666-670.

[5] S. Saqaeeyan and M. Roshanzadeh, “ Improved Energy Aware and Two Hop Multipath Routing Protocol in Wireless Sensor Networks”, *International Journal of Computer Network and Information Security*, 2012, Vol.5, pp.22-28.

[6] A.Senthilkumar and Dr.C.Chandrasekar, “Secure Routing in Wireless Sensor Networks: Routing Protocols”, *International Journal on Computer Science and Engineering*, Vol. 02, No. 04, 2010, pp.1266-1270.

[7] Hamid reza Hassaniasl, Amir masoud Rahmani, Mashaallah Abbasi Dezfuli & Arash Nasiri Eghbali, “A Novel Score-Aware Routing Algorithm in Wireless Sensor Networks”, *International Journal of Computer Science and Security (IJCSS)*, Volume 3, Issue 5, pp.397-404.

[8] Venkata Sumanth Mareedu, Sudheesha Cheepi and Venkata Durga Kiran Kasula, “Data Transferring Mechanisms for Multipath Routing Using Concentrated Dissimilate Algorithm in Wireless Networks”, *International Journal of Computer Trends and Technology*, Volume3, Issue1, 2012, pp.52-57.

[9] K. Saleem, N. Fisal, S. Hafizah, S. Kamilah, and R. A. Rashid, “A Self-Optimized Multipath Routing Protocol for Wireless Sensor Networks”, *International Journal of Recent Trends in Engineering*, Vol 2, No. 1, 2009, pp.93-97.

[10] Song Han, Zifei Zhong, Hongxing Li, Guihai Chen, Edward Chan and Aloysius K. Mok, “Coding-Aware Multi-path Routing in Multi-Hop Wireless Networks”, *IEEE Conference*, pp.93-100.

[11] Tanveer A. Zia and Albert Y. Zomaya, “A Lightweight Security Framework for Wireless Sensor Networks”, Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, volume: 2, number: 3, pp. 53-73.

[12] Wenjing Lou, “An Efficient N-to-1 Multipath Routing Protocol in Wireless Sensor Networks”, *IEEE conference*, 2005, pp.1-8.

[13] Ravindra Gupta & Hema Dhadhal, “Secure Multipath routing in Wireless Sensor Networks” *International Journal of Electronics and Computer Science Engineering*, Vol.1, No.2,2010, pp.585-589.

[14] Suraj Kumar Sharma & Sanjay Kumar Jena, “SCMRP: Secure Cluster Based Multipath Routing Protocol for Wireless Sensor Networks”, *IEEE Conference*, 2010, pp.1-6.

[15] Xiaoxia Huang& Yuguang Fang, “Multiconstrained QoS multipath routing in wireless sensor networks”, *Wireless Networks, Springer*, Vol.14, 2008, pp.465–478.

[16] Tao Shu, Marwan Krunz, and Sisi Liu, “Secure Data Collection in Wireless Sensor Networks Using Randomized Dispersive Routes”, *IEEE INFOCOM 2009 Mini-Conference*, 2009, pp.1-14.

[17] Wenjing Lou and Yuguang Fang , “A Multipath Routing Approach for Secure Data Delivery”, *IEEE Conference*, 2001, pp.1467-1473.

[18] Hannes Frey, Francois Ingelrest and David Simplot-Ryl, “ Localized Minimum Spanning Tree Based Multicast Routing with Energy-Efficient Guaranteed Delivery in Ad Hoc and Sensor Networks”, *Proceedings of IEEE conferences*, 2008, pp.1-8.

[19] Tapiwa M. Chiwewe, and Gerhard P. Hancke, “A Distributed Topology Control Technique for Low Interference and Energy Efficiency in Wireless Sensor Networks”, *IEEE Transactions On Industrial Informatics*, Vol. 8, No. 1, February 2012, pp.11-19.