International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-5S3, July 2019

Secure Routing with Improved Medium Access Control (SRI-MAC) Protocol for Wireless Sensor Network using Particle Swarm Optimization

N. Tamilarasi, S. G. Santhi

Abstract: ***A set of wireless sensor nodes comprises to form a sensor field called Wireless Sensor Networks (WSN).The main purpose of using the sensor node is to collect information from the ambience process it and send to a common gateway interface called Base Station(BS). The major problems that we face while using WSN are limited battery power, bandwidth, security issues and transmission delay etc. Many algorithms and protocols were developed in order to solve the above issues. Therefore, better solutions are required to face the improvements and challenges in the current technologies. In WSN, the sensor node highly loses its energy during communication period. One of the major issues of Medium Access Control (MAC) layer is collision. Collision increases the energy consumption and delay of the sensor node. So we have to conserve the energy of the sensor node in order to extend the lifetime of the network. At the same time it is also important to transmit the data through secure path and identify the malicious node. In this paper, we propose a novelty approach called Secure Routing with Improved Medium Access control (SRI –MAC) Protocol to solve the issues. SRI-MAC identifies packet precedence sets using Fuzzy Implication System (FIS) to avoid packet collision in MAC layer and also it detects wormhole attacks and selects secure path among k-paths using Particle Swarm Optimization (PSO) algorithm. By simulation results, we show that the proposed approach is efficient in terms of energy consumption and secure routing.***

Keywords: WSN, Fuzzy Implication System(FIS), Particle Swarm Optimization(PSO), MAC and Secure Routing with Improved –Medium Access Control (SRI-MAC).

I. INTRODUCTION

In the past few years, one of the most promising areas of research is Wireless Sensor Networks (WSN).These networks are used to monitor the environmental conditions such as temperature, pressure , vibration, sound, light etc., A wide range of WSN technologies are suitable for many real time applications like healthcare monitoring, environment monitoring, military, traffic surveillance and so on. Sensor nodes are being very small, it includes batteries, microcontroller, antenna and storage unit. The transmitting range depends on the device that is used to sense the ambience[1]. So it is very important to save the energy of the sensor node in order to prolong the life period of the network.

Manuscript published on 30 July 2019.
***** Correspondence Author (s)
N. Tamilarasi, Assistant Professor, HOD in the PG and Research Department of Computer Science, Sri Akilandeswari Women's college.
S.G.Santhi, Assistant Professor, Department of Computer Science & Engineering, Annamalai University.

If we conserve the energy means all the other parameters such as packet delivery ratio, throughput, extension of network lifetime and end to end delay can be possibly improved. So it is important to design a protocol for MAC layer in order to minimize the collision problems. Collision causes retransmission of data. This leads to high loss of energy[2]. Security problems dominate the sensor nodes while using Wireless network. There are many types of attacks which creates misbehavior attitude such as drops packets randomly, selective forwarding, eavesdropping and so on within the network[3]. The most crucial attack is Wormhole, which creates a tunnel path between source to destination. Two malicious nodes are placed as neighbor nodes for source and destination and create an illusion that it is the shortest path for transmitting data. However security issues and energy conservation plays a vital role in WSN[4][5]. To achieve these objectives, SRI-MAC protocol is proposed this paper.

A. Proposed Work

In this approach an enhanced MAC protocol is proposed and is designed based on the Fuzzy Implication System. Using this approach, packet precedence sets are identified based on the Enduring Delay and Enduring Buffer to avoid the packet collisions.

There are k number of paths are available to transmit data from source to destination. Among the *k* paths in the network, Wormhole attack free path is identified based on the detection packet.

This detection packet includes round trip time and hop-counts of the corresponding route. The source node sends detection packet to the destination node and it receives feedback packet from the neighbor nodes. Then the source node compares detection packet with the feedback packet. If the roundtrip time is less than the threshold round trip time and the hop-count is equals to 2, then the route is considered as the Wormhole attacked route and it is ignored. Otherwise, it is considered as active route.

After identifying the Wormhole route, optimal secure path is selected from the rest of the paths using PSO algorithm. In this algorithm, minimum threshold value is considered as the fitness function. The path with the minimum threshold value is considered as the most trusted and secured path for data transmission. This proposed approach is implemented in the Network Simulator (NS2). Performance of this proposed approach is evaluated in terms of QoS and energy consumption approach.

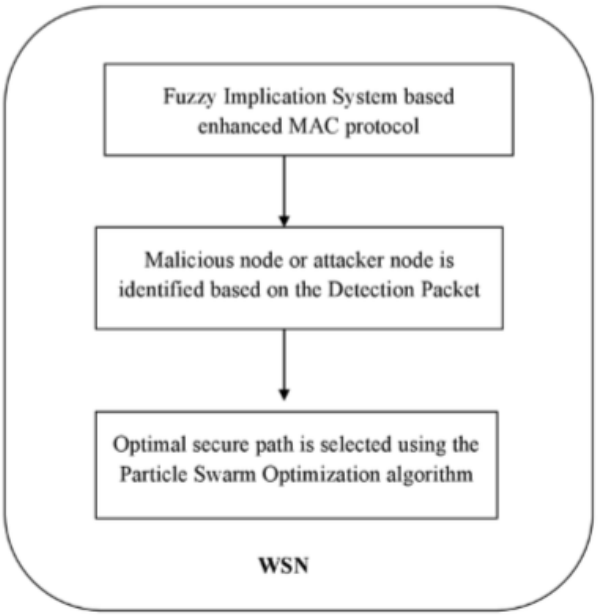


Fig.1 **Overview of the proposed approach**

II. RELATED WORK

Ashutosh Bhatia, R.C. Hansdah [6] proposed a TRM-MAC ,which is based on TDMA MAC protocol.The unique feature of this protocol is its ability to trade-off reliability performance for energy and delay depending upon the channel conditions and application. In addition to that it is reliable at the link layer and transport layer by creating multicast solution for reliable end to end delay.

N.Thangamani, S.John Grasias, Dr.G.Dalin [7] proposed the UCON-IPSO to detect the malicious activity and the Distributed Denial of Service .so they defined two techniques called Software Defined Networking(SDN) and Network Function Virtualization(NFV) for measuring the attacks. Abnormal traffic growth is monitored in the direction of server based on incoming traffic. As a result they demonstrated that their proposed work has higher security and attack detection rate.

Sunita Rani and Jaya [8] proposed a BFO-fuzzy rule based solution which identifies malicious node in order to reduce the data loss all over the network. They also provide the performance evaluation on various network parameters such as throughput, packet Delivery Ratio etc.,

E. Vaidhegi, C. Padmavathy, T. Priyanka and A. Priyadharshini [9] proposed a delay scheduling algorithm to improve the quality of service based on urgency metrics. To improve the throughput of the network node urgency, packet urgency and route urgency were chosen for the metric. To maximize the number of arriving packets, scheduling algorithm and routing algorithm are closely tied.

A. Ahmed, K. Bakar, M. Channa and A. Khan [10] proposed a Trust and Energy aware Secure Routing Protocol (TESRP) for detecting attackers in the network. It selects the shortest path by increasing the confidence and energy saving capacity of every node.

III.SECURE ROUTING WITH IMPROVED MEDIUM ACCESS CONTROL (SRI-MAC)

A.Fuzzy Implication System Based Enhanced MAC Protocol

MAC layer of the network is designed based on the Fuzzy Implication system. Using this system, packets which are to be transmitted in a node are given precedence based on the parameters Enduring Delay (ED) and Enduring Buffer (EB) [11][12]. In this algorithm, minimum of ED and EB is considered as Suitability Function (SF) to select packet which is to be transmitted first.

Suitability Function (SF) = min (ED + EB)

B. Enduring Delay(ED)

Enduring Delay at time t is calculated by subtracting the Cumulative Delay(CD) of source to i_{th} node from the maximum End to End Delay(EED).

$$ED(t) = EEDmax - CD_i(t)$$

EEDmax is the maximum endurable End to End Delay and $CD_i(t)$ represents Cumulative Delay from source to i_{th} node.

C. Enduring Buffer (EB)

Enduring Buffer of a node i is evaluated as dividing the Number of Packets in the Queue buffer(NPQ) of node i by the Total Buffer Size (TBS) of node i.

$$EB(i) = NPQ(i)/TBS(i)$$

Where NPQ(i) denotes Number of Packets in the i_{th} node Queue buffer and TB(i) represents the Total Buffer Size at node i.

The value of EB(i) is always in the range[0 ,1].

D . Fuzzy Implication System (FIS)

The concept of Fuzzy logic is based on “degrees of truth” quiet opposite to normal true or false(0 or 1). Because current generation computers support Boolean logic. Transformation of input space into an output space is done conveniently using fuzzy logic. Everything starts from this transformation of input to output. It is based on the examination that people make decisions based on incorrect and non-numerical data, fuzzy models or sets are mathematical means of representing imprecise information and vagueness, hence the term fuzzy[13]. These models have the capability of recognizing, representing, manipulating, interpreting, and utilizing data and information that are vague and lack certainty. The main motivation for using fuzzy logic is adaptive, fast and relatively simple implementation and it is less sensitive to system fluctuations. The procedure of transforming a crisp input value to a fuzzy value that is executed by the use of the data in the knowledge base. Fuzzification process commonly uses Gaussian, triangular and trapezoidal representation curves[14]. Fuzzy Implication System consists of five processes: (i) Fuzzification of the crisp inputs (ii) Apply Fuzzy operator in the ancestor (iii) Implication from the ancestor to the subsequent (iv) Aggregation of the consequents across the rules (v) Defuzzification.

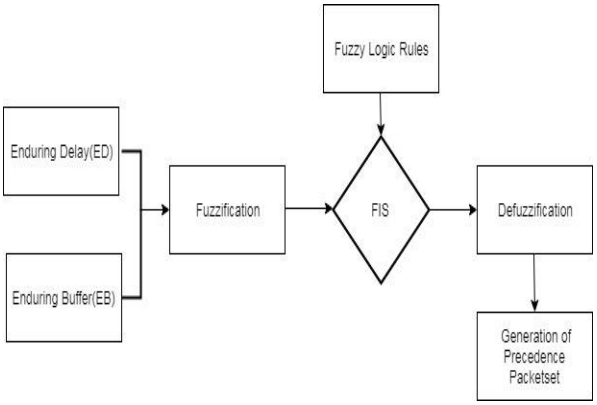


Fig.2 Fuzzy Implication System

S.No	ED	EB	SF
1	Min	Min	DVMin
2	Min	Avg	DMin
3	Min	Max	DAvg
4	Avg	Min	DMin
5	Avg	Avg	DAvg
6	Avg	Max	DMax
7	Max	Min	DAvg
8	Max	Avg	DMax
9	Max	Max	DVMax

Table .1 Fuzzy Rule

E. Fuzzification

In this paper, Fuzzification takes two crisp input values such as Enduring Delay(ED) and Enduring Buffer (EB). Fuzzification process maps the crisp inputs to corresponding fuzzy sets.

ED = Enduring Delay ∈ {Min, Avg, Max}

EB = Enduring Buffer ∈ {Min, Avg, Max}

The next step is to apply the inputs to the Fuzzy Implication System (FIS) and then it generates the fuzzy output set as follows:

Suitability Function (SF) ∈ {DVMin, DMin, DAvg,DMax, DVMax}

The output values represents five fuzzy states including: DVMin (Delay Very Minimum), DMin (Delay Minimum), DAvg (Delay Average), DMax (Delay Maximum) and DVMax (Delay Very Maximum). All the values should be in the range [1, 0].We used Gaussian function to represent these sets. The fuzzy number A = (a, b, c) is called Gaussian function is defined as

$$\mu_A(x) = \begin{cases} 0, & (x < a) \text{ or } (x > d) \\ \frac{x-a}{b-a}, & a \le x \le b \\ 1, & b \le x \le c \\ \frac{d-x}{d-c}, & c \le x \le d \end{cases}$$

F .Defuzzification Process:

Defuzzification is the method of minimizing a fuzzy set to a crisp single valued quantity. so we must find out the minimum value between μ(ED) and μ(EB) and we are using AND logic in order to write fuzzy rules.

$$\mu(ED \cap EB) = \min(\mu ED, \mu EB)$$

G.Identification of Malicious Node:

1. Note the time as T1_k for each route request transmitted by source node where k represents number of paths .
2. Note the time as T2_k for each route reply acknowledged by the source node where k represents number of paths.
3. The round trip time for all routes is determined by using the formula

   RTT_k = T2_k - T1_k
4. The threshold round trip time for all the k paths can be calculated by using the formula

   TRTT_k = RTT_k/HC_k
5. The average threshold round trip time for all the k paths are calculated by using the following formula :

   ATRTT_k = TRTT_1+TRTT_2+TRTT_3+…….+TRTT_k/k

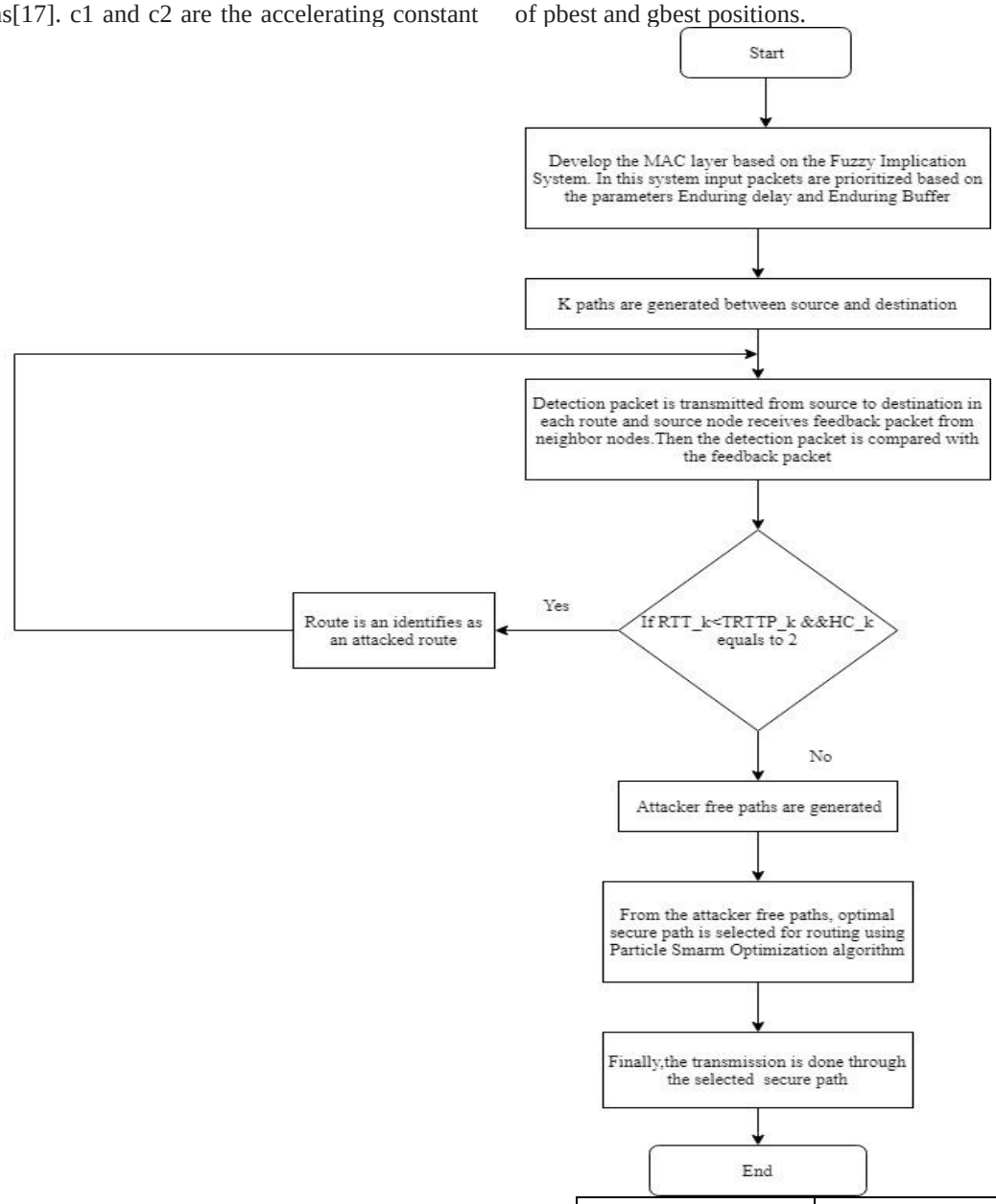
   The above calculated ATRTT_k is called threshold round trip time for the network.

6. if((TRTT_k<ATRTT_k)&&(HC_k = 2)) then
   {
   a. Route k is identified as wormhole attacked path.
   b. The first neighbor node M1 after the source node is declared as wormhole node
   c. The first neighbor node M2 after the destination node is also declared as wormhole node.
   d. A dummy RREQ packet is sent through route k from source to destination via M1 and M2.
   e. The malicious node M1and M2 are removed from the routing table and also advertised to further nodes in the network.
   }
   else `
   {
   The route is confirmed as attacker free route.
   }
   end If

H.Selection of optimal Secure path Using PSO:

In 1995Dr. Kennedy and Dr. Eberhart developed a population based stochastic optimization technique called Particle swarm optimization (PSO),motivated by social behavior of fish schooling or bird flocking. PSO is an ease, efficient and computationally well- organized optimization algorithm. It has been applied to address WSN issues such as node localization, clustering, data-aggregation and optimal deployment[15][16].PSO is initialized with a collection of arbitrary particles and then finds for most favorable solution by revising generations. For each iteration, every particle is updated by following two "best" values. The solution that is achieved so far is called the pbest value. The value that is tracked by the particle swarm optimizer is called the gbest value.

At each step PSO modifies the velocity of each accelerating particle in the direction of its pbest and gbest locations[17]. c1 and c2 are the accelerating constant which corresponds to the weighting of the stochastic acceleration term that drags each particle in the direction of pbest and gbest positions.



IV.SIMULATION RESULTS

A.Simulation Setup

The proposed SRI_MAC (Secure Routing with Improved Medium Access Control) is implemented using Network Simulator NS2. 250 sensor nodes are simulated in the region 1000m X 1000m.The Transmission capability of each sensor node in the wireless network is 0.66W and the receiving capability is 0.395W. Interference range of the sensor node is 550m, Omni directional antenna in two way propagation. Constant Bit Rate is used as a traffic source in the entire wireless network. Nodes transmit their information in the form of packets. The storing capacity of each packet is 1024 bytes and it is transmitted at the rate of 80 kbps with the simulation time of 100 sec. Table 2 shows the simulation structure.

Simulation Structure

No. of Nodes	50, 100, 150, 200, 250
Area Size	1000m X 1000m
MAC TYPE	MAC / 802_11
Propagation	Two Ray Ground
Antenna	Omni Antenna
Interference range	550 m
Transmission Range	250m
Simulation Time	100 sec
Traffic Source	CBR
Packet Size	1024 bytes
Rate	80 kbps

Table.2 Simulation structure

B.Performance Evaluation based on Nodes:

The proposed SRI-MAC approach is examined by changing the number of nodes as 50,100,150,200 and 250. Figures 3 – 5 shows the comparison of performance evaluation based on number of nodes between the proposed SRI-MAC and existing TRM-MAC.

Figure 3 represents the comparison of Network Life Time between the SRI-MAC and TRM-MAC. When the number of nodes in the network increases, life time of the network is decreases for the existing TRM-MAC by 17% compared to SRI-MAC. Packet Delivery Ratio is increased by 14% when the number of nodes in the network increases and it is shown in the figure 4.Energy consumption of the SRI-MAC decreases by 12% when the number of nodes in the network increases as shown in the figure 5.

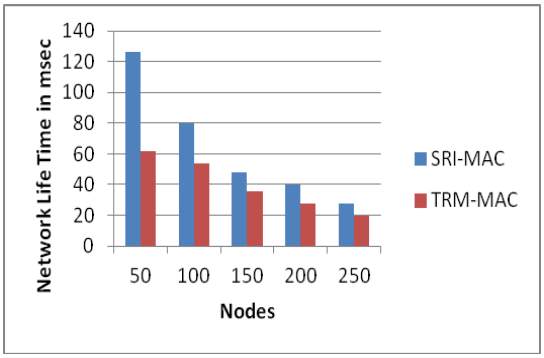


Fig.4 Nodes Vs NLT

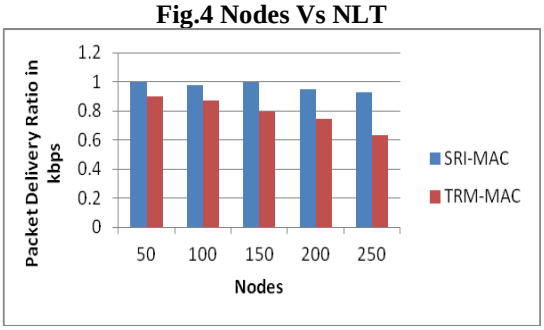


Fig.3 Nodes Vs PDR

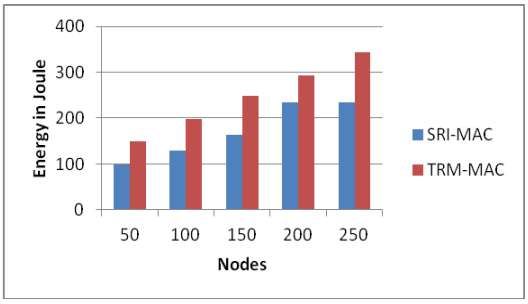


Fig.5 Nodes Vs Energy

C. Performance Evaluation Based on Speed

The proposed SRI-MAC approach is examined by changing the transmission speed as 10,20,30,40 and 50 Mbps. Figures 6 – 8 shows the comparison of performance evaluation based on speed between the proposed SRI-MAC and existing TRM-MAC. Figure 6 represents the comparison of Network Life Time between the SRI-MAC and TRM-MAC. When the speed of the network increases, life time of the network is decreases for the existing TRM-MAC by 14% compared to SRI-MAC. Packet Delivery Ratio is increased by 15% when the speed of the network increases and it is shown in the figure 7.Energy consumption of the SRI-MAC decreases by 20% when the speed of the network increases as shown in the figure8.

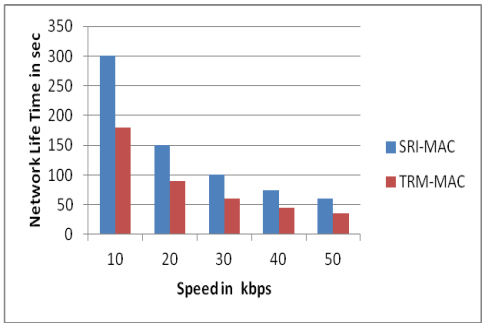


Fig.6 Speed Vs NLT

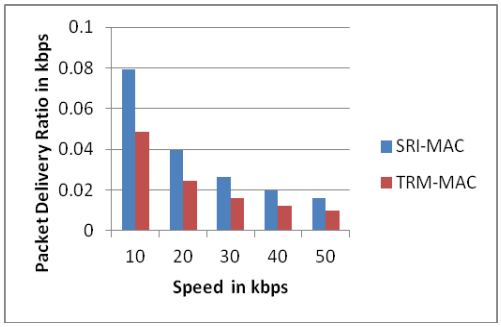


Fig.7 Speed Vs PDR

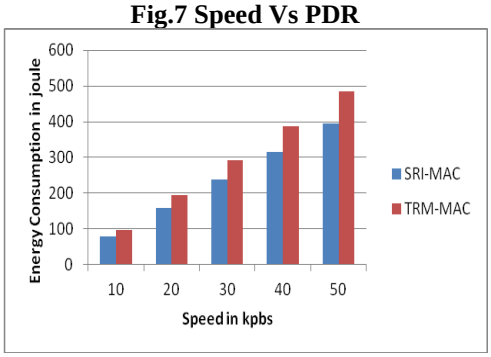


Fig.8 Speed Vs Energy

V. CONCLUSION

In this paper, Secure Routing with Improved Medium Access Control(SRI-MAC) is presented. Using this proposed mechanism, energy conservation and collision problems has been solved in the MAC layer itself by calculating the suitability function based on Fuzzy Implication System(FIS).FIS takes two crisp inputs Enduring Delay and Enduring Buffer to identify the precedence packets. Then discovery of malicious activity especially Wormhole attack is detected using Round Trip Time and Threshold Round Trip Time. Finally attacker free k paths are identified. Among the k paths , optimal secure routing is selected using PSO algorithm in order to transmit the data from source to destination in a secure and optimal way. Simulation results showed that the performance of the proposed SRI-MAC outperformed that of the existing TRM-MAC in terms of energy consumption, packet delivery ratio and network lifetime. Furthermore this proposed work can be extended by preventing the Wormhole attack in addition to detection. Because prevention of attack is very essential for Wireless Sensor Networks.

REFERENCES

1. C. Y. Wan, S. B. Eisenman, and A. T. Campbell, "CODA: congestion detection and avoidance in sensor networks," in Proceedings of the first International Conference on Embedded Networked Sensor Systems, pp.266–279, CA, USA, Nov 2003.
2. [M. A. Kafia, D. Djenourib, J. B. Othmanc, A. Ouadjaouta, and N.Badachea, "Congestion detection strategies in wireless sensor networks: a comparative study with testbed experiments," Procedia Computer Science, vol. 37, pp. 168–175, 2014.
3. A. Mohajerani and D. Gharavian, "An ant colony optimization based routing algorithm for extending network lifetime in wireless sensor networks", Wireless Networks, vol. 22, no. 8, pp. 2637-2647, 2015..
4. Prabha VR, Latha P. Enhanced multi-attribute trust protocol for malicious node detection in wireless sensor networks. Sadhana. 2017 Feb 1; 42(2):143-51.
5. M. Hatamian, H. Barati, and A. Movaghar, "A new greedy geographical routing in wireless sensor networks," Journal of Advances in Computer Research, vol. 6, no. 1, pp. 9–18, 2015.
6. A. Bhatia and R. Hansdah, "TRM-MAC: A TDMA-based reliable multicast MAC protocol for WSNs with flexibility to trade-off between latency and reliability", Computer Networks, vol. 104, pp. 79-93, 2016.
7. N.Thangamani, S.John Grasias, Dr.G.Dalin "Ucon-Ipso: Usage Control with Improved Particle Swarm Optimization (Ipso) Based Hierarchical Security Framework for Attack Detection in Wireless Sensor Networks" IJETST- Vol.||04||Issue||08||Pages 5681-5691||August||ISSN 2348-9480
8. Sunita Rani and Jaya "Wireless Sensor Network: Black Hole Attack Detection Using BFO-FUZZY" International Journal of Computer Science and Mobile Applications, Vol.3 Issue. 9, September- 2015, pg. 42-52
9. E. Vaidhegi, C. Padmavathy, T. Priyanka and A. Priyadharshini , " Delay Sensitive Packet Scheduling Algorithm for MANETs by Cross Layer", IJIRAE – International Journal of Innovative Research in Advanced Engineering, vol .1,Issue 1,2014
10. Ahmed, K. Bakar, M. Channa and A. Khan, "A Secure Routing Protocol with Trust and Energy Awareness for Wireless Sensor Network", Mobile Networks and Applications, vol. 21, no. 2, pp. 272-285, 2016.
11. J. Wei, B. Fan, and Y. Sun, "A congestion control scheme based on fuzzy logic for wireless sensor networks," in Proceedings of the 9th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD 2012), pp. 501–504, Sichuan, China, May 2012.
12. O. B. Akan, and I. F. Akyildiz, "Event-to-sink reliable transport in wireless sensor networks," IEEE/ACM Transactions on Networking, vol.13, no. 5, pp. 1003–1016, 2005.
13. Ewa Niewiadomska-Szynkiewicz and Filip Nabrdalik, "Secure Low Energy AODV Protocol for Wireless Sensor Networks", ITNAC – International Telecommunication Networks and Applications Conference , 2017.
14. S. Sarang, M. Drieberg, A. Awang and R. Ahmad, "A QoS MAC protocol for prioritized data in energy harvesting wireless sensor networks", Computer Networks, vol. 144, pp. 141-153, 2018.
15. Binitha S, "A Survey of Bio inspired Optimization Algorithms" International Journal of SoftComputing and Engineering ISSN: 2231-2307, Volume-2, Issue-2, May 2012.
16. Kiran Narang, "Black Hole Attack Detection using Fuzzy Logic" International Journal of Science and Research, Volume 2 Issue 8, August 2013.
17. Yash Pal Singh, "A Survey on Detection and Prevention of Black Hole Attack in AODV- based MANETs" journal of information, knowledge and research in computer engineering, nov 12 to oct 13 ,volume – 02, issue – 02.

AUTHOR BIOGRAPHY:

The author N.Tamilarasi is Working as an Assistant Professor and HOD in the PG and Research Department of Computer Science at Sri Akilandeswari Women's college – Wandiwash. She is having ten years of teaching and Research experience in the field of Computer Science. She has completed her B.Sc., Computer science from Shanmuga Industries Arts & Science college – Tiruvannamalai. M.C.A., and M.Phil., Computer science from Annamalai University – Annamalai Nagar. B.Ed from Pondicherry University – Pondicherry.And also she has Passed State level eligibility test(SET) in the year 2012 and National Eligibility test (NET) in 2018.she has published thirteen international journals.Currently she is doing Ph.D at Annamalai University.

. Dr.S.G.Santhi obtained her Bachelor's degree in Computer Science & Engineering from Moogambigai College of Engineering, Bharathidasan University in 1992 then she obtained her Master's degree in CSE from Annamalai University in 2005. She received her Ph.D in Computer Science & Engineering from Annamalai University in 2005. She is currently working as an Assistant Professor in the Department of Computer Science & Engineering,Faculty of Engineering and Technology – Annamalai University. She is having 19 years of experience in teaching. She has published 14 Research papers in International journals and more than 10 International and National Conferences. Her field of interest includes Wireless Sensor Networks and Internet of Things. She is currently guiding 4 research scholars towards Ph.D. She is a life member in various professional bodies like ISTE,CSI etc.