Secure Optimal Path Using Swarm Intelligence Advanced ACO Routing Technique in WSN

R.N.S. Kalpana, M. Jagruthi

Asst.prof, Dept. of ECE, Teegala Krishna Reddy College of Engg and Technology, Meerpet, Hyderabad

Abstract- In wireless sensor networks, the upsides of manhandling the sink portability to drag out system lifetime have been particularly seen. In physical circumstances, an extensive variety of obstacles could exit in the distinguishing field. Wireless Sensor Networks comprising of hubs with constrained power are sent to assemble helpful data from the field. In WSN, it is basic to gather the data in an effective way. WSN is a gathering of little, huge number of thickly conveyed sensor hub; these sensor hubs are keen, successful which is great and flexible systems administration where customary wired and remote systems administration can't send. Trust aware routing is significant for both securing achieved data and additionally shielding the system execution from degradation and system assets from absurd utilization because of insider attacks in wireless sensor systems. This paper presents Normal ACO method (Ant Colony Optimization) protocol for WSN. This protocol is supportable to wireless networks with some secure levels but doesn't overcome the malicious impact in network process. So we proposed a new technique called SA-ACO with QoS parameters (link quality, distance and energy with trust values). It improves the routing ways, giving a powerful data transmission to get dependable interchanges on account of malicious node distinguishes. The fundamental objective is to keep up the ideal way, amid data transmission in an effective way. Our simulation outputs comes about show that SA-ACO performs amazingly well as far as malicious nodes moderation, packet delivery ratio, end to end delay, energy utilization and throughput. Simulation results through NS2 software to verify the effectiveness of our method.

I. INTRODUCTION

Many research works have focused on the security of WSNs. A large portion of them [4] manage counteractive action and recognition ways to deal with individual getting out of hand nodes. In such manner, the viability of these methodologies winds up frail when different malicious nodes conspire together to start a synergistic attack, which may result to all the more wrecking damages to the system. In DDoS attacks, the approaching activity flooding the casualty starts from a wide range of sources. This viably makes it difficult to stop the attack just by blocking a solitary source. In order to appreciate the concept of Trust aware routing, one needs to consider some aspects that highlight the importance of Trust based routing. Firstly, misbehaving nodes in a wireless sensor network can indulge in misrouting packets to wrong destinations leading to misinformation or can deny totally forwarding packets to their destination leading to loss of information. Mission critical applications such as military, health or commercial applications can be very sensitive to these attacks where WSN nodes have the utmost responsibility to carry and deliver very critical and secret information. Hence, it becomes highly essential to design a Trust aware routing protocol to protect data exchange, secure information delivery and maintain and protect the value of the communicated information.

In Trust aware routing, the opinion of a node about the behavior of its next forwarder node is considered in the routing decision. This opinion is quantified and termed as Trust metric which should reflect how much a forwarder is expected to behave to forward a packet when it receives from its previous node in the path from source to sink. The calculation of trust metric is independent from anyone else a test as it requires a few operational assignments on watching nodes conduct, trading nodes' involvement and opinions and additionally demonstrating the gained perceptions and traded information to reflect nodes trust esteems. A system that performs these tasks to ultimately generate suitable trust rating for nodes is called a reputation system [1]. A notoriety system is a sort of helpful filtering calculation which endeavors to decide evaluations for a gathering of elements that have a place with a similar network [2, 3]. Every entity rates other entities of interest based on a given collection of opinions that those entities hold about each other. Reputation systems have received considerable attention in different fields such as distributed artificial intelligence, economics, evolutionary biology, e-commerce applications and online auctioning, ad hoc and wireless sensor networking, etc. Most of the concepts in reputation systems depend on social networks analogy. In general, any reputation system in the context of WSN should consist of three main components– Monitoring, Rating and Response. Monitoring component is responsible for observing the activities of the neighbor nodes. Rating component will enable the nodes to rate their neighbor nodes based on the node's own observation, other nodes' observations that are exchanged among themselves, the history of the observed node and certain threshold values. Response component has the responsibility of deciding about different possible reactions it can take, like avoiding bad nodes or even punishing they based on the knowledge built by nodes on others' reputations.

Swarm Intelligence research has been largely carried out to reverse engineer and adapt properly the collective behaviors observed in natural systems such as ant colonies, flocks of birds and schools of fishes to design novel algorithms for distributed optimization and Control [4]. Ant Colony systems have effectively handled the difficulties postured by the nature utilizing their intrinsic engaging qualities, for example, adjusting to varying ecological conditions, powerful and strong to the disappointments caused by inner or outer variables, accomplishing complex practices and shared task based on a restricted arrangement of standards and compelling administration of obliged resources with global insight which is bigger than singular abilities [5]. Similarities could be drawn with ant colony systems when one considers many of the significant challenges to be addressed in practical realization of wireless sensor networking solutions such as resource constraints, absence of centralized control and infrastructure, complexity and dynamicity of large scale networks, need for survivability and self-configurability, and lastly unattended resolution of potential failures.

In this paper, the system paths should be strong it means like optimal paths considered. Keeping these in mind, pheromone update model has been designed considering the parameters the forward ant has collected during its travel from source to the destination, i.e., trust rating of the path, available average Energy, minimum energy of the nodes along the path, Number of hops, and link quality of the path to reinforce a path with enough pheromone to select that path as the best path to reach the sink from the source.

II. RELATED WORK

In this section, we present some of the related work carried out in the area of Trust-aware routing for wireless sensor networks. Recent work demonstrates that the advantage utilizing the trust aware of nodes has been well recognized. By using the trust aware of nodes in WSNs, we can easy to set the optimal paths and enhance energy efficiency for nodes. Henceforth, the system lifetime is extended significantly. Many papers have proposed several different approaches. We then study the related works of the trust aware of nodes in the literature.

Reputation system based framework for Energy Efficient, Trust-enabled Secure Routing for wireless Sensor Network is proposed in [1, 6-10]. This work proposes a customized reputation system-Sensor Node Attached Reputation Evaluator (SNARE)[6,7]. SNARE is a collection of protocols and algorithms that interacts directly with the network layer. The system adopts the geographical routing principle to cope with large network dimensions and relies on a distributed trust management system for the detection of malicious nodes. The system consists of three main components; i.e. monitoring component, rating component and response component. The monitoring component, EMPIRE (Efficient Monitoring Procedure in Reputation system) [8, 10], observes packet forwarding events. Here a monitoring node will not be in a continuous monitoring mode of operation, rather, it will monitor the neighborhood periodically and probabilistically to save resources. At the point when a misbehaving event is recognized, it is tallied and put away until the point when a refresh time and after that a report is sent to the rating segment. Therating part, CRATER (Cautious Rating for Trust Enabled Routing) [9], assesses the measure of hazard a watched node would accommodate steering activity. The hazard esteem is an amount that speaks to the past acting mischievously exercises that a malicious node got. This esteem is utilized as a desire for how much hazard would be endured by choosing that defective node as a switch. It is calculated based on the first hand information and the second hand information.

In the Basic Ant Colony Optimization (ACO) based routing algorithm for WSN [11], along with the data traffic, forward ants are launched at regular intervals from source node with the mission to locate the sink node with equal probability by using neighbor nodes with minimum cost along the path from source to sink. At each intermediate node, the forward ants use a greedy stochastic policy to choose the next node to travel. During the travel, the forward ants collect information (such as distance, delay, congestion status and the node identifiers) of the followed path. Once the destination is reached, forward ants die and backward ants are created which take the same path as the forward ants, but in an opposite direction whose mission is now to update the pheromone trail of the path the forward ants used to reach the destination. Amid this regressive travel, nearby models of the system status and the neighborhood directing table of each went to hub are adjusted by the retrogressive ants as a component of the way they took after and of its integrity. When they have come back to their source hub, the regressive ants die.

III. HYBRID ALGORITHM

In this segment, we exhibit our proposed system SA-ACO with Distance, Energy, Link quality, Trust values, and Key generation. We shall introduce advanced clustering mechanism in previous work so we should follow cluster-based algorithm for clustering and cluster head selection that works with ACO. Here all the communications are directed through cluster head (CH) to sink (receiving node). We can setup secure mechanism to increase the security during routing; we introduce a method based on Secure Elliptical Curve Cryptography (SECC). The model is shown in figure 1 which consists of three main components –Clustering phase, Swarm advanced ACO and Secure ECC which are discussed next.

A. Trust setup

In Trust Model, nodes rate each other by using the information of their own direct interactions with their neighbors. This is termed in the literature as First Hand Information (FHI). In order to make the rating unbiased, the nodes also collect their neighbors' interactions with that node being rated considered as indirect interaction. This rating information collected from the neighbors is also known as Second Hand Information (SHI). The simulation period is now divided into 'n' slots where each slot consists of two sub-periods -Forwarding and Monitoring Interval, TFMI followed by Update Interval TUPI as shown in Table1.

Initialization Phase	T_F MI	T_U PI	T_F MI	T_U PI	…	T_F MI	T_U PI	. .	T_F MI	T_U PI

Table1: Simulation period slots

B. Forwarder selection function

Forwarder Selection Function is a probability function that is used at every node along the path from source to sink node in the network to select the best next neighbor to forward the packet to the sink node. The Forwarder Selection Function must always choose an optimal path from source to the sink to forward the packets with the sole objective to improve the Network Lifetime by balancing the energy among the nodes in the network to ensure that some nodes along the path do not get depleted fast and at the same time selecting good quality links along the path to guarantee that node energy is not wasted due to too frequent retransmissions.

C. Pheromone Model

It has been observed that the amount of pheromone computed to be placed on the path during return journey is not proper to reflect that path as the optimal during the simulation period. Strongest path should have largest amount of pheromone whereas weakest path should have least amount of pheromone or almost zero. Among the competing stronger paths for selection, the variations in pheromone concentration should be such that always strongest path is selected.

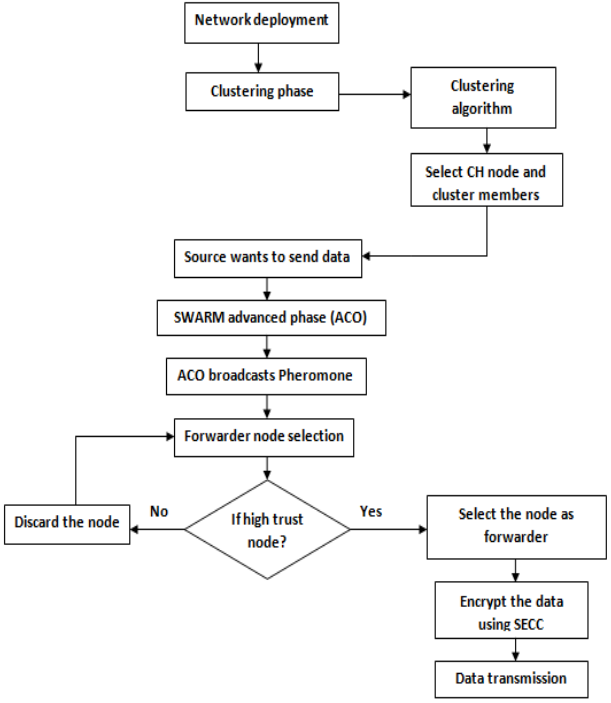


Fig.1: SA-ACO Framework

D. Algorithm:

Step1: Initialization of network process

Step2: Source node request for destination based on selection procedure for hop nodes

Step3: Randomly place ant nodes in network

Step4: Build the location of destination

Step5: Using forwarder selection procedure and select the routes for knowing path for sending the data

Step6: Check the all neighbor nodes for select the best routing path

Step7: There are two working models for the ants: either forward or backwards

Step8: The ant node memory allows them to retrace the path it has followed while searching for the destination node

Step9: Before moving backward on their memorized path, they eliminate any routes form it. While moving backwards, the ants leave pheromone on the arcs they traversed.

Step10: Here trust model can support to knowing the individual node probability.

E. Secure ECC Mechanism

In this mechanism, each and every node has its own unique keys (public, private keys). The node should have a valid key to transmit the data. Here network process; malicious nodes have invalid keys. So they cannot participate in the communication further. We can apply ECC (Elliptical Curve Cryptography) then overcome the malicious node activity.

- **Generation key management**

The public key and the private key are generated specifically in the key generation. Encrypting the message by the sender with the receiver's public key and decrypting its private key by the receiver.

We can generate the public key by selecting a number**'d'** within the range of **'n'** and using the following equation

$$Q = d * p \text{……….}1$$

d= the random number within the range of (1 to n-1) which is selected; 'P' is the curve-point.

'Q' is the public key and'd' is the private key.

- **Encryption**

For message sending let us consider 'm'. The message on the curve has to be represented. These have in-depth implementation details.

On the curve 'E' let us consider 'm' has the point, 'M'. Randomly select 'k' from [1-(n-1)].

Let C_1 and C_2 be the two cipher texts that will be generated.

$$\{C_1 = k * p, C_2 = M + k * p\} \text{……………}2$$

C_1 And C_2 will be sending.

- **Decryption**

The message 'm' that was sent to us, has to get back

$$M = C_2 - d * C_1 \text{……………}3$$

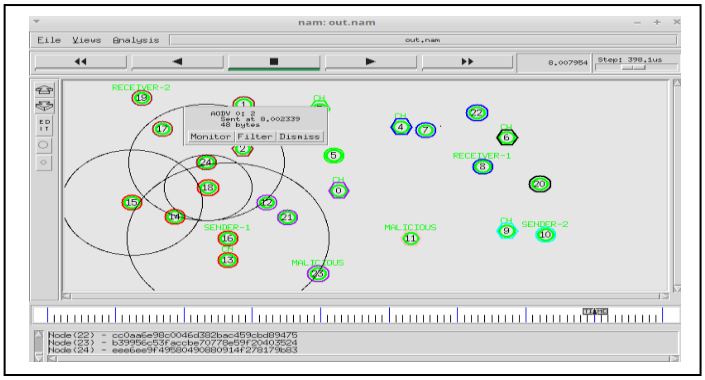
M is the original message that we have send.

IV. EXPERIMENTAL RESULTS

In this paper, we assume that 25 sensor nodes are randomly distributed over a 1000x500m^2 field where different random way points setup. In this paper, we have considered static network scenario with nodes randomly distributed. Our proposed trust enabled routing approach SA-ACO is compared with ACO and Normal AODV without network failure using 25nodes by introducing 10%, 20% and30% non-forwarding attackers in the network. The performance evaluation metrics used in the simulation are Packet Delivery Ratio, End to End Delay, Dropping Ratio and Throughput. Table2 shows the system parameters used in our simulations. In this paper,

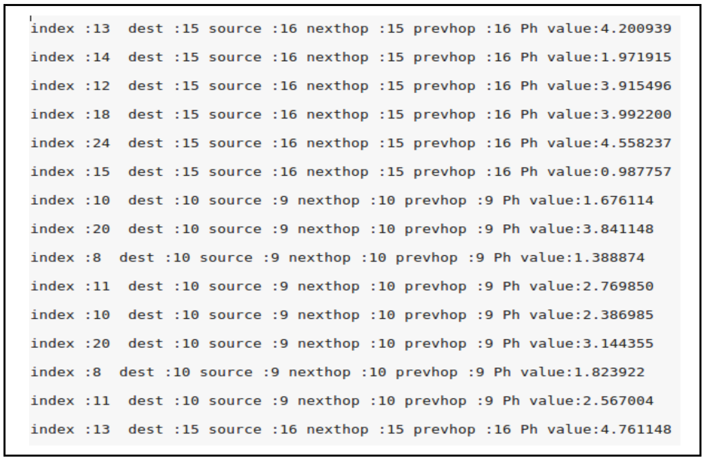
PARAMETER	**VALUE**
Application Traffic	CBR
Transmission rate	15 packets/sec
Radio range	250m
Topology	Random
Propagation model	Two way ground
Packet size	512 bytes
Maximum speed	25m/s
Simulation time	9000ms
Number of nodes	25
Area	1000x500
Clusters	8
Initial energy	100j
Routing protocol	SA-AODV
Maximum packets	10000
Malicious nodes	3

Table2: System parameters



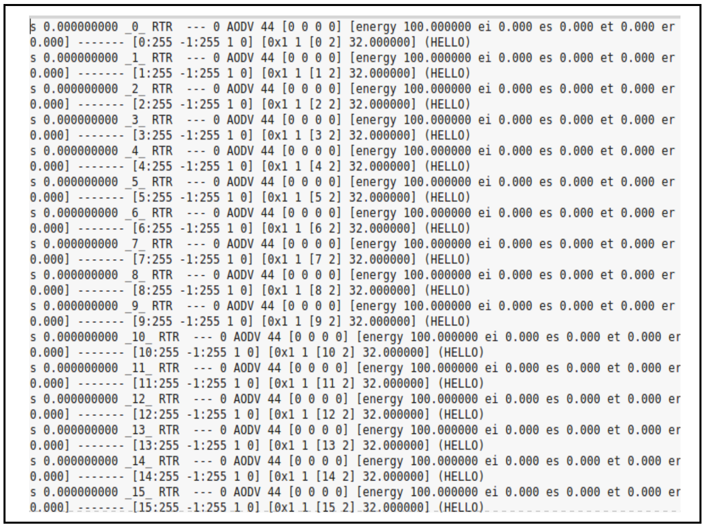
```
Node(22) - cc0aa6e98c0046d382bac459cbd89475
Node(23) - b39956c53faccbe70778e59f20403524
Node(24) - eee6ee9f49580490880914f278179b83
```

Figure 2: Routing process in N/W



```
index :13  dest :15 source :16 nexthop :15 prevhop :16 Ph value:4.200939
index :14  dest :15 source :16 nexthop :15 prevhop :16 Ph value:1.971915
index :12  dest :15 source :16 nexthop :15 prevhop :16 Ph value:3.915496
index :18  dest :15 source :16 nexthop :15 prevhop :16 Ph value:3.992200
index :24  dest :15 source :16 nexthop :15 prevhop :16 Ph value:4.558237
index :15  dest :15 source :16 nexthop :15 prevhop :16 Ph value:0.987757
index :10  dest :10 source :9 nexthop :10 prevhop :9 Ph value:1.676114
index :20  dest :10 source :9 nexthop :10 prevhop :9 Ph value:3.841148
index :8  dest :10 source :9 nexthop :10 prevhop :9 Ph value:1.388874
index :11  dest :10 source :9 nexthop :10 prevhop :9 Ph value:2.769850
index :10  dest :10 source :9 nexthop :10 prevhop :9 Ph value:2.386985
index :20  dest :10 source :9 nexthop :10 prevhop :9 Ph value:3.144355
index :8  dest :10 source :9 nexthop :10 prevhop :9 Ph value:1.823922
index :11  dest :10 source :9 nexthop :10 prevhop :9 Ph value:2.567004
index :13  dest :15 source :16 nexthop :15 prevhop :16 Ph value:4.761148
```

Fig.3: Phenomenon values with Hops



```
s 0.000000000 _0_ RTR  --- 0 AODV 44 [0 0 0 0] [energy 100.000000 ei 0.000 es 0.000 et 0.000 er
0.000] ------- [0:255 -1:255 1 0] [0x1 1 [0 2] 32.000000] (HELLO)
s 0.000000000 _1_ RTR  --- 0 AODV 44 [0 0 0 0] [energy 100.000000 ei 0.000 es 0.000 et 0.000 er
0.000] ------- [1:255 -1:255 1 0] [0x1 1 [1 2] 32.000000] (HELLO)
s 0.000000000 _2_ RTR  --- 0 AODV 44 [0 0 0 0] [energy 100.000000 ei 0.000 es 0.000 et 0.000 er
0.000] ------- [2:255 -1:255 1 0] [0x1 1 [2 2] 32.000000] (HELLO)
s 0.000000000 _3_ RTR  --- 0 AODV 44 [0 0 0 0] [energy 100.000000 ei 0.000 es 0.000 et 0.000 er
0.000] ------- [3:255 -1:255 1 0] [0x1 1 [3 2] 32.000000] (HELLO)
s 0.000000000 _4_ RTR  --- 0 AODV 44 [0 0 0 0] [energy 100.000000 ei 0.000 es 0.000 et 0.000 er
0.000] ------- [4:255 -1:255 1 0] [0x1 1 [4 2] 32.000000] (HELLO)
s 0.000000000 _5_ RTR  --- 0 AODV 44 [0 0 0 0] [energy 100.000000 ei 0.000 es 0.000 et 0.000 er
0.000] ------- [5:255 -1:255 1 0] [0x1 1 [5 2] 32.000000] (HELLO)
s 0.000000000 _6_ RTR  --- 0 AODV 44 [0 0 0 0] [energy 100.000000 ei 0.000 es 0.000 et 0.000 er
0.000] ------- [6:255 -1:255 1 0] [0x1 1 [6 2] 32.000000] (HELLO)
s 0.000000000 _7_ RTR  --- 0 AODV 44 [0 0 0 0] [energy 100.000000 ei 0.000 es 0.000 et 0.000 er
0.000] ------- [7:255 -1:255 1 0] [0x1 1 [7 2] 32.000000] (HELLO)
s 0.000000000 _8_ RTR  --- 0 AODV 44 [0 0 0 0] [energy 100.000000 ei 0.000 es 0.000 et 0.000 er
0.000] ------- [8:255 -1:255 1 0] [0x1 1 [8 2] 32.000000] (HELLO)
s 0.000000000 _9_ RTR  --- 0 AODV 44 [0 0 0 0] [energy 100.000000 ei 0.000 es 0.000 et 0.000 er
0.000] ------- [9:255 -1:255 1 0] [0x1 1 [9 2] 32.000000] (HELLO)
s 0.000000000 _10_ RTR  --- 0 AODV 44 [0 0 0 0] [energy 100.000000 ei 0.000 es 0.000 et 0.000 er
0.000] ------- [10:255 -1:255 1 0] [0x1 1 [10 2] 32.000000] (HELLO)
s 0.000000000 _11_ RTR  --- 0 AODV 44 [0 0 0 0] [energy 100.000000 ei 0.000 es 0.000 et 0.000 er
0.000] ------- [11:255 -1:255 1 0] [0x1 1 [11 2] 32.000000] (HELLO)
s 0.000000000 _12_ RTR  --- 0 AODV 44 [0 0 0 0] [energy 100.000000 ei 0.000 es 0.000 et 0.000 er
0.000] ------- [12:255 -1:255 1 0] [0x1 1 [12 2] 32.000000] (HELLO)
s 0.000000000 _13_ RTR  --- 0 AODV 44 [0 0 0 0] [energy 100.000000 ei 0.000 es 0.000 et 0.000 er
0.000] ------- [13:255 -1:255 1 0] [0x1 1 [13 2] 32.000000] (HELLO)
s 0.000000000 _14_ RTR  --- 0 AODV 44 [0 0 0 0] [energy 100.000000 ei 0.000 es 0.000 et 0.000 er
0.000] ------- [14:255 -1:255 1 0] [0x1 1 [14 2] 32.000000] (HELLO)
s 0.000000000 _15_ RTR  --- 0 AODV 44 [0 0 0 0] [energy 100.000000 ei 0.000 es 0.000 et 0.000 er
0.000] ------- [15:255 -1:255 1 0] [0x1 1 [15 2] 32.000000] (HELLO)
```

Fig.4: trace file of N/W

Figure 2 indicating key generation process of network. Here calculate public key and private keys of all trusted nodes and setup with network based upon key representation it called as elliptical curve cryptography. Figure 3 shows calculation and printing data of Phenomenon values. The Figure 4 represents trace file of our proposed system from network initialization to end of network process. All nodes, variables, values, parameters, routing levels, time variation based on process including and all trace from proposed framework network animator (NAM). Here this trace file indicates as output file of network.

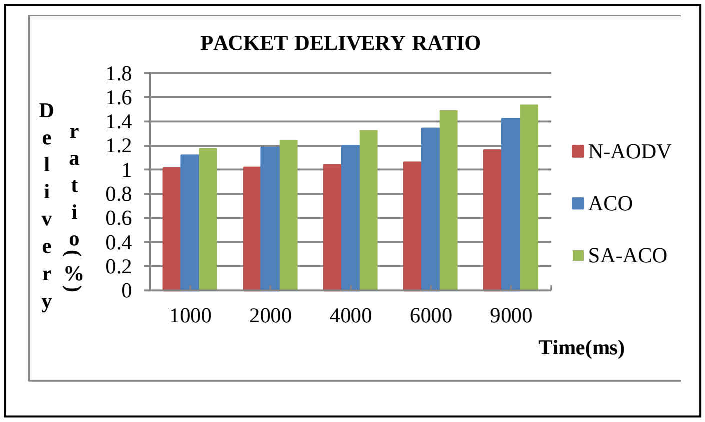


Fig.5: Network Packet delivery ratio

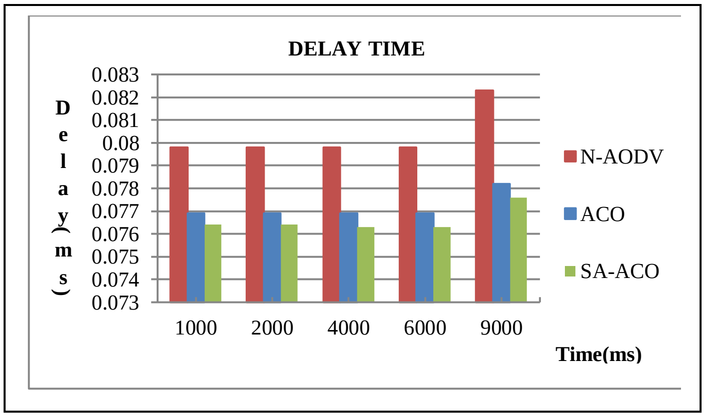


Fig.6: Routing delay performance

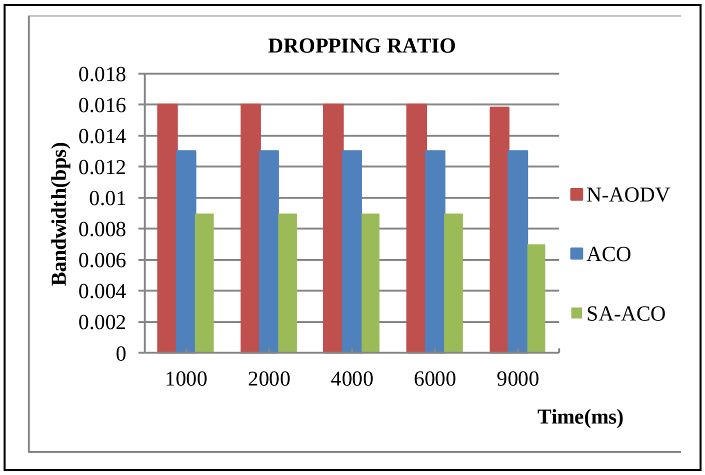


Fig.7: Dropping ratio

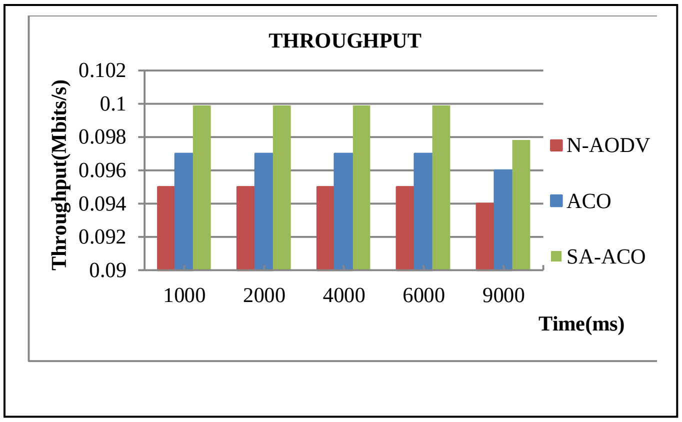


Fig.8: Network performance

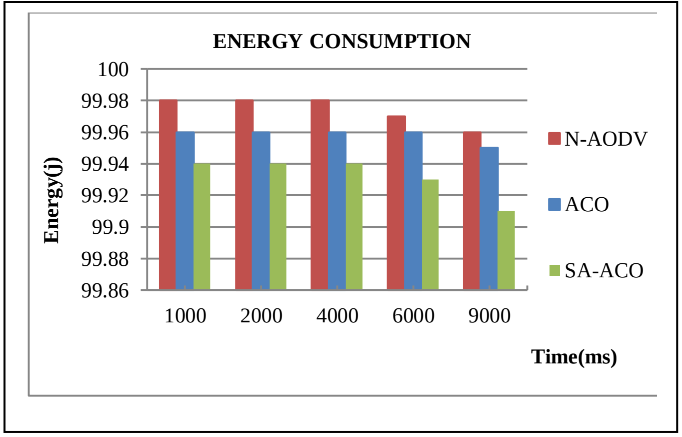


Fig.9: Energy consumption

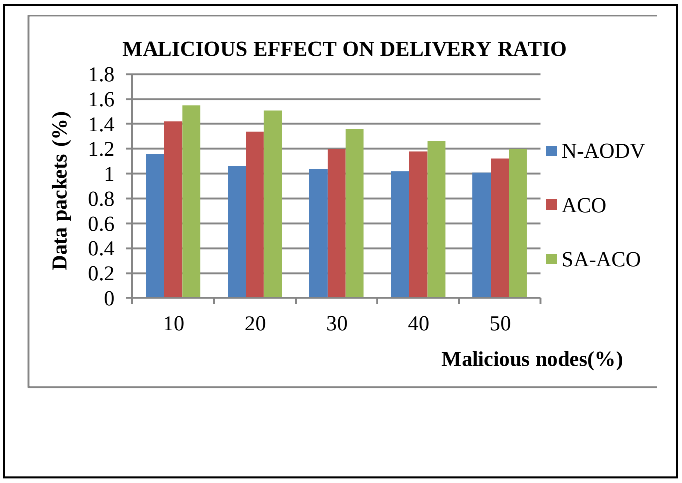


Fig.10: Delivery ratio by malicious effect

In Figure 5, graph represents packet delivery ratio in network. Here graph represents simulation time versus delivery of packets. In this graph, shows comparison of our proposed method with existing approaches named as Normal-AODV and ACO. In Figure 6, graph shows and represents end2end delay and it shows a simulation time versus delay. The performance of SA-ACO method improves delay time it means decrease the delay between communications nodes compare to Normal-AODV and ACO. Figure 7 graph represents dropping ratio in network. Here graphical representation simulation time versus dropping packets. In this graph, we compare our proposed method with Normal-AODV and ACO approaches. Figure 8 shows and represents throughput and it shows a simulation time versus throughput. The performance of SA-ACO method improves the throughput compare to Normal-AODV and ACO. Figure 9 shows and represents energy consumption and it shows a simulation time versus energy. The performance of SA-ACO method improves energy values compare to Normal-AODV and ACO. Figure 10 represents malicious impact on delivering the packets. Here graph shows that malicious nodes versus delivered packets. And it has shown the malicious effect on network process. The delivering of packets gradually decreases but compare to existing approaches our proposed system is better.

V. CONCLUSION

In this paper, we have presented our proposed model SA-ACO, Swarm Intelligence Ant colony optimization with Distance, Energy, Link quality and Trust Awareness. In SA-ACO, routing decisions are based on ACO methodology which incorporates Trust, Remaining Energy, Distance, and Link quality attributes to choose the best next hop for the routing operation, thus allowing for better load balancing and network lifetime extension. The secure way of routing depends on key distribution of keys. We also conducted simulation by using NS2 and exploratory outcomes demonstrate that our SA-ACO is practical for the discriminate Malicious and improve ACO with a secure mechanism. We finally overcome malicious activity based on trust values with Normal ACO method.

VI. REFERENCES

[1]. A. R. Naseer, “Reputation System based Trust-Enabled Routing for Wireless Sensor Networks”, published in Handbook of Research on Wireless Sensor Networks, INTECH Open Access Publisher, USA, 2012.

[2]. P. Resnick, R. Zeckhauser, E. Friedman, and K. Kuwabara, “Reputation systems: Facilitating trust in internet interactions,” Comm. of the ACM, vol. 43, no. 12, pp. 45–48, 2000.

[3]. T. Grandison and M. Sloman, “A survey of trust in internet applications,” IEEE Comm. Surveys & Tutorials, vol. 3, no. 4, 2000.

[4]. Gowrishankar. S, T.G.Basavaraju, Manjaiah D.H, Subir Kumar Sarkar, Issues In Wireless Sensor Networks, WCE 2008.

[5]. M. Dorigo, and G.A. Di Caro (1998). “AntNet: Distributed stigmergetic control for communications networks”, *Journal of Artificial Intelligence Research.* vol. 9, pp. 317–365, 1998.

[6]. V. Neelima , A.R. Naseer , “SIBER-DELTA: **S**warm Intelligence Based Efficient Routing with Distance, Energy, Link quality and Trust Awareness for Wireless Sensor Networks “ , International journal of scientific and engineering research , Volume 7, Issue 7, July-2016.

[7]. I. K. Maarouf and A. R. Naseer, “WSNodeRater: An optimized Reputation System Framework for Security Aware Energy Efficient Geographic Routing in WSNs”, in Proceedings of ACS/IEEE International Conference on Computer Systems and Applications, AICCSA ‘2007, May 13-16, 2007 Amman, Jordan

[8]. A. R. Naseer, I.K. Maarouf, U. Baroudi, , “Efficient Monitoring Approach for Reputation System based Trust-aware Routing in Wireless Sensor Networks”, International Journal of IET Communications –Wireless Adhoc Networks, May 2009, Volume 3, Issue 5, pp. 846-858, ISSN 1751-8628.

[9]. I.K. Maarouf, U. Baroudi, A. R. Naseer, “Cautious Rating for Trust-enabled Routing in Wireless Sensor Networks”, EURASIP International Journal on Wireless Communications and Networking, 2010, Volume 2, Article ID 718318, 16 pages, ISSN: 1687-1472.

[10]. A. R. Naseer, “EMPIRE –Energy Efficient Trust-Aware Routing for WSN”, Hand book of Research on Dynamic Ad Hoc Networking, IET Publisher, UK/USA, 2013.

[11]. M. Dorigo, and G.A. Di Caro (1998**).** “Ant Net: Distributed stigmergetic control for communications networks”, Journal of Artificial Intelligence Research. vol. 9, pp. 317–365, 1998.