International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 18 (2017) pp. 7052-7067

Lifespan Enhanced Energy Efficient Cluster Formation and Trusted Multipath Data Transmission for Packet Forwarding in Wireless Sensor Network

[1]R. Gopinathan [2]Dr.P. Manimegalai

[1]Research Scholar, Department of Electronics and Communication Engineering
Karpagam University, Karpagam Academy of Higher Education,
Coimbatore – 641 021, Tamil Nadu, India.

[2]professor, Department of Electronics and Communication Engineering,
Karpagam University, Karpagam Academy of Higher Education,
Coimbatore – 641 021, Tamil Nadu, India.

Abstract

Due to unwanted overheads observed in security process of WSNs, the time consumption of each node is very high from authentication, key generation and key distribution phases. Hence every data packet experiences the same latency. The efficiency of exchanging the secret key degrades rapidly as a function of external signal interference power and limits its resilience against active attackers. Moreover, the latency in the network is also increased since Secret Key (SK) value is refreshed for every session. Hence it could be seen that any increase in the strength of data security is achieved at the cost of overhead utilization in the network. In Reliable Anonymous Secure Packet forwarding (RASP) scheme, a total of 44 bytes packet size, 20 bytes of authentication message size and 20 bytes for data transmission (160 bits) are used. Hence, the number of transmission is increased, which in turn increases the control overhead and traffic at the network and demands for secret key during each transmission. To overcome the above issues, a multipath routing protocol, based on the clustering algorithm, is proposed in this research paper. Moreover, Particle Swarm Optimization (PSO) is used in cluster formation in order to optimize intra-cluster and sink distance of the entire cluster heads (CHs), which subsequently reduces the energy consumption in WSNs. For an enhancement of network life time and security, the trust values of each node in the cluster formation and head selection process are considered. The trust values are calculated from the trust inference model (i.e., dolphin echolocation algorithm). Finally, the trusted clustering model is combined with the standard multipath routing protocol (i.e. AOMDV) to analyze the performance and security issues. The simulated result shows that the proposed scheme performs better than RASP scheme. The network lifetime of the proposed work is increased by 10%, 8%, and 15% than RASP scheme. The delay of proposed work is decreased by 5%, 3%, and 5% as compared to RASP scheme. The energy consumption of proposed work is decreased by 10%, 5%, and 4% than RASP scheme. The delivery ratio of proposed work is decreased by 5%, 5%, and 5% than RASP scheme.

Keywords: Particle Swarm Optimization (PSO), Clustering, Cluster heads (CHs), Trust, Ad hoc on-demand Multicast Distance Vector protocols (AOMDV), dolphin echolocation algorithm.

INTRODUCTION

Wireless Sensor Networks (WSNs) consist of spatially distributed and independent sensors for checking physical conditions such as, dampness, temperature, sound, weight, light, unstable natural mixes etc. Sensor nodes in the system are equipped with memory, a radio frequency transceiver and a power source. They skim the data as packets/messages remotely over a specified protocol [1]. Packet forwarding is a typical means for sensor nodes to proficiently impart their packets to one another. The packet forwarding mechanism can be used to introduce the system plan for route discovery between a given pair of senor nodes and could serve as a productive strategy to confine sensor nodes. Packet forwarding maximizes the packet delivery ratio and minimizes the rate of packet loss. The major advantage of this technique is the maximization of delivery ratio and reduction of energy cost simultaneously.

The cluster based packet forward technique [2-4], a reliable and energy-efficient forwarding REEF [2], selects one node among receivers in cluster for broadcasting packets from nodes in sender node to present cluster. The selected node sends an acknowledgment (ACK) back to the sender node present in cluster and broadcasts the packet to nodes in neighboring cluster. In secure data forwarding for cluster-based WSNs (CWSNs), clusters are formed dynamically and periodically. There are two secure and efficient data transmission (SET) protocols for CWSNs, called SET-IBS and SET-IBOOS, by using the Identity-Based Digital Signature (IBS) scheme and the Identity-Based Online/Offline digital Signature (IBOOS) scheme, respectively [3]. The Distributed Similarity based Clustering and Compressed Forwarding for wireless sensor networks construct data

similar intra clusters with minimal communication overhead. The cluster head reduces the inter cluster data payload using a lossless compressive forwarding technique [4]. Check point based Multi-Hop Acknowledgement Scheme (CHEMAS) [5] for detecting selective forwarding attacks in packet forwarding process and weighted Localized Delaunay Triangulation based data forwarding techniques (WLDT) [6], is used for extending the network lifetime.

Some other routing protocols are used for maximizing the energy efficiency [7-11]. An adaptive sleeping [7] in which each node selects its relay based on a new criterion based on its residual energy resources and its geographical location is also found to guarantee energy efficiency in the literature. Two forwarding schemes termed single-link and multi-link energy efficient forwarding that trade off delivery ratio against energy costs [8] are also investigated in the literature. An efficiency diversity driven by selective forwarding scheme [9] is used to solve the problems where the detected object fails to match the tuples held at the local sensor. The low latency end-to-end paths in wireless link quality also play a significant role in the performance of packet forwarding. Expected transmission delay (ETD) [10] formation determines the sleep latency and wireless link quality. Simple selective policies with Information-Driven Sensor Querying (IDSQ) scheme combined with energy efficient schemes, such as data aggregation or data fusion schemes used to improve the network lifetime [11].

For security reason key management scheme based data forwarding protocols [3] [12] [13] are proposed that are aware of security issues. Bandwidth efficient cooperative authentication (BECAN) scheme for filtering injected false data saves energy by early detection and filtering of the majority of injected false data with minor extra overheads at the en-route nodes [12]. A reliable anonymous secure path forwarding scheme (RASP) for traffic attacks and compromised forwarding nodes protects the communication in WSN by providing anonymous secure communication to a greater extent [13]. In RASP approach, three steps are being carried out for a reliable communication between the sensor node and the base station (BS): (1) one hop and two hop node selection and table formation for route establishment between sensor node and BS. (2) Key generation at BS and transmitted to the sensor node through authentication reply message. (3) Authenticated session setup for the secured data forwarding. The limitations of RASP approach are present as follows:

1. Time consumption at each node is very high (during authentication, key generation and key distribution); hence, every data packet experiences the same latency.
2. The efficiency of exchanging the secret key degrades rapidly as a function of external signal interference power and limits its resilience against active adversaries. Since Secret key (SK) value is refreshed for every session to increase the security strength of the data communicated, the overhead utilization in the network increases rapidly.
3. For a total of 44 bytes packet size, 20 bytes of an authentication message and 20 bytes for data transmission (160 bits), the number of transmission is increased, which in turn increases the control overhead and traffic at the network and demands for Secret Key during each transmission.

The proposed multipath data forwarding schemes provides the energy efficient and secure path for data transmission in wireless sensor networks. A multipath data forwarding schemes with two stage transmission route is established. The first stage is to form the cluster [2-4] and select the cluster head (CH) based on practical swarm optimization (PSO) [14] among nodes in that cluster. Then in second stage the security of route is enhanced by trust based multipath routing scheme [15]. The proposed scheme is simulated over a large number of sensor nodes with a wide range of mobility and the performance is evaluated and compared with the existing routing protocols. The main contributions of the proposed work are as follows:

1. Given the need of cluster formation and cluster head selection, cluster formation is carried out to optimize intra-cluster and sinks distance of all the CHs, to save energy in wireless sensor network.
2. A trust based multipath routing model is abstracted, where an entity for an interest neighbor forms the basic building block of the model. Using the node status of each node in WSNs the probability of congestion is reduced. Even if congestion occurs in the network, the traffic load of the congested node is reduced by splitting the traffic flow through an alternative path. Here the energy consumption during packet loss is minimized by hop-by-hop recovery scheme.
3. The performance evaluation shows that the proposed multipath packet forwarding scheme provides a secure and energy efficient network and also improves its life time, energy consumption and packet drop ratio and reduces end to end delay.

The remaining paper has been organized as follows. Section 2 discusses the related works of clustering and trusted routing protocols. Section 3, describes energy efficient and secure cluster formation, cluster head selection and trust calculation algorithms in detail. Section 4 analyzes the performance of the proposed cluster and trust based multipath routing protocol. Finally, Section 5 gives the concluding remarks of this paper.

RELATED WORKS

Several routing protocols have been proposed for data forwarding in WSN. In recent years the data forwarding protocols are designed based on the different methods. In the current case clustering and trust estimation are used. This section discusses the recent related works similar to the proposed work based on clustering, cluster head (CHs) selection and trusted multipath routing in WSNs.

Ahmed Bader *et al.* [16] proposed position based protocols for data forwarding scheme that was variation in node density and the protocol was so designed that it took out the requirement for potential relays to experience a hand-off determination process. The operation of this protocol was

enabled by using positive components of orthogonal frequency division multiplexing (OFDM) at the physical layer. The end-to-end execution of the protocol was assessed against beaconless position-based protocols logically. The protocol's fundamental righteousness was that it did not fall back on any hand-off determination process. At any given hop, potential relays checked whether they fulfilled certain position based criteria. Any relay that satisfied the criteria chose to forward the bundle ahead. It did so without returning any kind of coordination with other potential transfers. At the terminals of accepting nodes, such a system would, without a doubt, make various duplicates of the same packets with various propagation delays.

Ju Ren *et al.* [17] proposed a Channel- aware Reputation System with adaptive detection threshold (CRS-A) to identify specific sending assaults in WSNs. The system lifetime was arranged by an arrangement of assessment periods. During every assessment period, sensor nodes appraised the typical packet loss rates amongst themselves and their neighboring nodes, and received the evaluated packet loss rates to assess the sending behaviors of its downstream neighbors along the data forwarding path. The sensor nodes acting mischievously in data forwarding were rebuffed with diminished notoriety values by CRS-A. Once the notoriety estimation of a sensor hub was beneath a caution esteem, it would be recognized as a bargained hub by CRS-A.

Yong Zhang *et al.* [18] solved the asymmetrical communication energy consumption problem by using the concept of evolution game theory and the method of adjusting the CH selection probability based on evolution stable strategy. Authors used the Territory game (TGC algorithm) to define the area limits in clustering algorithm. TGC algorithm mitigated the unbalanced energy consumption caused by the asymmetrical distance from CHs to the sink. Game based clustering algorithms used to obtain evolution stable strategies when considering the sensors asymmetrical distance to the sink and remaining energy.

Ren-Cheng Jin *et al.* [19] proposed distributed passive cluster-based multipath routing protocol for WSNs. A scalable and distributed passive clustering algorithm based on smart delay strategy, which depended on the energy levels and the distances was investigated, which organized the entire network into clusters. N-to-1 multipath routing algorithm was used to obtain multiple paths from each cluster head (CHs) node to the base station. Authors introduced path cost to conduct the selection of optimal paths, by which each cluster head node might remain multiple paths to the base station.

Tao Du *et al.* [20] analyzed the energy efficiency in a typical hierarchical routing algorithm. The hierarchical algorithm named as Energy Efficiency Semi-Static Clustering (EESSC) which was based on the improved Hierarchical Agglomerative Clustering (HAC) clustering approach. EESSC algorithms, the sensor nodes residual energy would be taken into account in clustering operation, and a special packet head was defined to help update the node energy information when transmitting message among the nodes. When the clusters had been formed, the nodes in cluster would be arrayed in a list and cluster head would be rotated automatically by the order of list. And a re-cluster mechanism was designed to dynamic adjust the result of clustering to make sensor nodes organization more reasonable.

Shilpa Mahajan *et al.* [21] selected the CHs based on the performance of parameters like weight metric and then cluster formation took place in a random network. The number of nodes that could be accommodated in the cluster without degrading network performance was considered. For uniform load distribution and a local clustering mechanism, cluster head rotation could take place within the cluster and that too when some specific condition was met.

Gokce Hacioglu *et al.* [22] proposed a multi-objective optimization algorithm namely non dominated Sorting Genetic Algorithm-II (NSGA-II), which was used for the transmission of the message collected within them to sink by cluster heads. The total energy required for non-cluster-heads to send messages directly to sink, inverse total energy of cluster heads, total energy required for non-cluster-heads to send message to the cluster heads and total energy of nodes which were non cluster head had been investigated and computed in the research work.

Suraj Sharma *et al.* [23] addressed the idea to reduce the load of the sensor node by giving more responsibility to the base station, and it gathered neighboring station information from the sensor nodes and created a neighbor adjacency matrix. The sink node identified the cluster head and selected the appropriate path. The base station sent the paths to the elected cluster heads. Each cluster head built its cluster and sent the aggregated data to the sink. If routing path failed between cluster head and the sink, the sink selected another path for data transmission. The sink monitored the residual energy of each node and based on that, balanced the load among the sensor nodes.

Shiva Murthy *et al.* [24] proposed sink initiated proactive protocol called secure Energy Efficient Node Disjoint Multipath Routing Protocol (EENDMRP) for WSNs. It found multiple paths between the source and destination based on the rate of energy consumption and filled queue length of the node. The security threats to the WSN like spoofing or altering the route information, selective forwarding, sinkhole attack, Sybil attack and byzantine attack were addressed. It provided more security by using the digital signature crypto system. The data packets were transmitted in a secure manner by using the digital signature crypto system i.e. MD5 hash function and RSA algorithm.

Liu *et al.* [25] formulated secret sharing based disjoint multipath routing optimization problem. Authors increased the security and life time of network by delivery of sliced packet shares along randomly generated disjoint paths by the routing scheme. They considered the network security and lifetime to frame the security and energy-efficient disjoint route (SEDR). Here the packets are divided into different slices using the threshold secret-sharing algorithm and the

divided slices are randomly forwarded to all the nodes including the sink node in the networks using least hop routing.

PROPOSED MULTIPATH DATA FORWARDING METHOD

This section first discusses the concept of the cluster formation and cluster head selection, based on optimization algorithm, and is based on trust and distance parameters. The trust weight vector selection parameters and algorithm have been discussed briefly in this section.

Structure of Cluster Formation and Clustering Parameters

Actually, grouping sensor nodes into clusters has been broadly received by the research group to fulfill the adaptability objective and by and large accomplish high energy effectiveness and draw out system lifetime in large scale WSN environments. In the hierarchical network structure every cluster has a head, which is called the cluster head (CH) and normally plays out the tasks with a few sensor nodes (SN) as members. A normal case of the implied hierarchical data communication within a clustered network is further illustrated in fig. 1. The BS is the data processing point for the data received from the sensor nodes, and where the data is received by the end user.

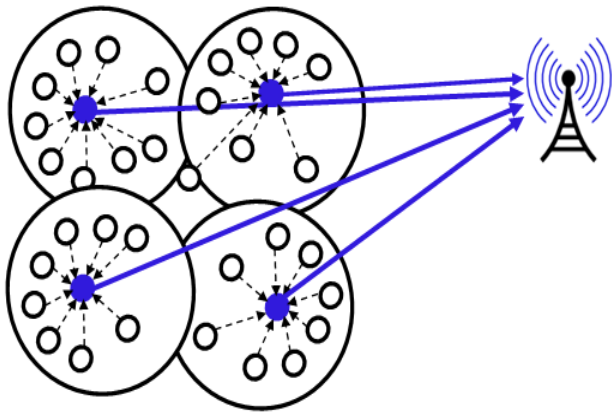

Figure 1. Structure of Clustering with Cluster Head

It is for the most part viewed as settled and at a far distance from the sensor nodes. The CH nodes really act as gateway between the sensor nodes and the BS. The function of each CH is similar to the normal functions, like every one of the hubs in the clusters, such as accumulating the information before sending it to the BS. Somehow, the CH is the sink for the cluster nodes, and the BS for the CHs. Besides, the structure shaped between the sensor nodes, the sink (CH) and the BS can be recreated as many times as required to make the various layers of the hierarchical WSNs. Some general parameters are required for cluster formation in the network such as cluster count, Intra cluster communication, Nodes and CH mobility, Nodes type and roles, Cluster formation methodology and cluster head selection. The proposed approach consists of CH selection and cluster formation. The CH selection is based on PSO and the algorithm is based on sensor node trust value and distance parameter. The entire paper considers the node terminologies and set of sensor nodes or and cluster heads are denoted by $S = \{s_1, s_2, \cdots, s_n\}$ and $CH = \{CH_1, CH_2, \cdots, CH_m\}$ respectively with $m < n$. The fitness value is calculated for choosing a cluster head depends on the following three factors namely,

1. Intra cluster and sink distance of CHs
2. Energy of current selected CHs
3. Trust value of CHs

Cluster Head Selection Based On PSO Algorithm

Particle Swarm Optimization (PSO) is an algorithm [28-29] to problems whose solutions can be represented as a point in an n-dimensional solution space. A number of particles are randomly set into motion through the space and the fitness value of own and their neighbors, at each iteration and are observed to emulate successful neighbors by moving towards them. The grouping particles are computed by different schemes; semi-independent flocks are used or all the particles can belong to a single global flock. PSO was developed by James Kennedy and Russell in 1995 [26] after being inspired by the study of bird flocking behavior by biologist. PSO starts with a group of random particles and then searches for optimal by updating generations, each particle being updated by following two best values. The first best solution (fitness) is called P_{best}, another best value is called global best i.e. g_{best} is tracked by PSO and obtained so far by any particle in the population.

$$p_{best_k} = \begin{cases} p_k, & If\ \left(fitness(p_k) < fitness\left(p_{best_k^i}\right)\right) \\ p_{best_k}, & otherwise \end{cases} \quad (1)$$

$$g_{best_k} = \begin{cases} p_k, & If\ \left(fitness(p_k) < fitness\left(g_{best_k^i}\right)\right) \\ g_{best_k}, & otherwise \end{cases} \quad (2)$$

A particle takes part in the population as its topological neighbors and the best value is a local best and is called I_{best}. Mathematically, swarm of particles is initialized randomly over the search space and moved through dimensional space to determine new solution. The position P_K^i and velocity V_k^i of i^{th} particle at the k^{th} iteration, then its velocity and position of this particle at $(K+1)^{th}$ iteration are updated by using (3) and (4).

$$V_{k+1}^{i} = \omega.V_k^i + c_1.rand_1.(p_{best_k^i} - P_k^i) + c_2.rand_2.(g_{best_k} - P_k^i) \quad (3)$$

$$P_{k+1}^{i} = P_K^i + V_{k+1}^i \quad (4)$$

Where ω is inertia weight, constant C_1, C_2 representing the learning factors normally equal to 2, and $rand_1$ and $rand_2$ represents random numbers between 0 and 1.

Delay Model: The delay model used in the paper is based on Average intra cluster distance (D_{IC}) [14] which is defined as the average of the sum of the distances of all the sensor nodes from their selected CH.

$$D_{IC} = \frac{1}{I_x}\sum_{y=1}^{I_y} dis(S_y, CH_x) \quad (5)$$

Average sink distance (D_s) is defined as the ratio of distance between a cluster head and the base station to the number of sensor nodes.

$$D_s = \frac{1}{I_x} dis(CH_x, BS) \quad (6)$$

In intra cluster and routing phase, all sensor nodes consume some energy to send data to their CH and it is required to route their aggregated data to the BS [30]. In order to consume less energy, it is necessary to reduce this average intra-cluster communication distance in intra cluster communication and select CH, which is close to all the sensor nodes. Minimization of the average intra-cluster and sink distance of all the CHs by optimal selection approach is achieved as

$$f_1 = \sum_{x=1}^{m}(D_{IC} + D_s) \quad (7)$$

Energy Model: The energy model used in this paper is based on the energy model implemented in [14] based on [26, 31, 33]. The transmitter and receiver dissipate energy to run the radio electronics and the power amplifier. The energy consumption of the node depends on the amount of the data and distance to be sent. The energy consumption of a node is proportional to square of distance (D^2) when the propagation distance (D) less than the threshold distance (D_0), otherwise it is proportional to (D^2) [14]. The total energy consumption of each node in the network for transmit and receive the n bit data packet is given in (8).

$$E_{total} = E_t(n, d) + E_r(n) \quad (8)$$

Where $E_t(n, d)$ and $E_r(n)$ are energy consumption of transmitting and receiving node.

$$E_t(n,d) = \begin{cases} n \times E_{elec} + n \times \varepsilon_{fs} \times D^2; \ if\ D < D_0 \\ n \times E_{elec} + n \times \varepsilon_{mp} \times D^4; \ if\ D \geq D_0 \end{cases} \quad (9)$$

$$E_r(n) = n \times E_{elec} \quad (10)$$

Where E_{elec} the energy is dissipated per bit to run the transmitter or receiver circuit, amplification energy for free space model (ε_{fs}) and for multi-path model (ε_{mp}) depends on the transmitter amplifier model and D_0 is the threshold transmission distance [32]. The total current energy (E_{CH_x}) of $CH_x; 1 \leq x \leq m$ is selected from the normal sensor nodes in iteration. The total current energy of all the selected CHs:

$$E_{total_{CH_x}} = \sum_{x=1}^{m} E_{CH_x} \quad (11)$$

The process of selecting optimal cluster heads is maximizing the total current energy of all the selected CHs [29]. Minimization of the current energy of the selected CHs is achieved by it is reciprocal:

$$f_2 = \frac{1}{\sum_{x=1}^{m}(E_{CH_x})} \quad (12)$$

Trust Inference Model: Dolphin Echolocation Algorithm [31] is an optimization algorithm which is used to determine the efficient node involved in a path. Dolphins primarily investigate all around the search space to discover the prey. The moment a dolphin approaches the target, the animal confines its search, and incrementally, increases its clicks in order to concentrate on the location. The method simulates dolphin echolocation by restraining its exploration relative to the distance from the target. A route with a better link quality is selected for forwarding data from source to destination. If a better link quality is not found, DEA function is performed again until global best solution has been found. DEA reduces the traffic and routing overhead of the optimization process and finds the node with best link quality in WSNs.

In the search space order every variable is to be optimized by sort alternatives of the search space in an uphill or downhill order. If alternatives take account of more than one characteristic, then ordering is carried out according to the most significant one. Using this technique, for variable x, vector A_x of length LA_x is shaped which contains all probable alternatives for the x^{th} variable putting these vectors subsequently to each other, as the columns of a matrix, the Matrix Alternatives $M_A + M_V$ is produced, in which M_A is $\max(LA_x)_{x-1:NV}$, with NV being the number of variables. Furthermore, a curve according to which the convergence factor must change during the optimization

procedure should be assigned. Here, the change of convergence (CF) is considered as

$$PP(loop_y) = PP_y + (1 - PP_1)\frac{loop_y^{power} - 1}{(loop_{snumber})^{power} - 1} \quad (13)$$

Where PP predefined probability is PP_1 is convergence factor of the first loop and $loop_y$ is the number of current loop. The detailed procedure of dolphin echolocation algorithm (DEA) starts with the N_L locations for a dolphin arbitrarily. This step encloses created $L_{N_L+N_V}$ matrix, in which N_L is the number of locations and N_V is the number of variables and to compute the predefined probability of the loop using (13). Initialize nodes i.e. number of echolocations in a MANET.

To compute the fitness (14) of each location of dolphin based on following search space dimension (15) and a position (16) equation.

$$Z(y) = fitness(P_y) \quad (14)$$

$$\pi_y(t+1) = \pi_y(t) + C_1(P_{Best} - P_y(t)) + C_2(G_{Best} - P_y(t)) \quad (15)$$

$$P_y(t+1) = P_y(t) + \pi_y(t+1) \quad (16)$$

where P_{Best} and G_{Best} is the personal and global best position found in dolphin, y is the search space index, t is the discrete time index and C_1, C_2 are random number i.e. [0, 1].

Then to compute the accumulative fitness according to dolphin rules such as (1) for x = 1 to the number of variables (2) for y = 1 to the number of locations (3) determine the position from the column of the alternative matrix m with $t = -R_e \; to \; R_e$.

$$PF_{A_{(m+t)_x}} = \frac{1}{R_e}(R_e - |t|)\, fitness(P_y) + F_{A_{(m+t)_x}} \quad (17)$$

Where $PF_{A_{(m+t)_x}}$ is the accumulative fitness of the $(m+t)^{th}$ alternative to be chosen for the x^{th} variable R_e is the effective radius in which accumulative fitness of the alternative neighbors is affected from its fitness P_y. PF_A is calculated from reflective characteristics i.e. in order to hand out the option much evenly in the search space, a small value of ε is added to all the arrays as $PF_A = PF_A + \varepsilon$. Here, ε should be selected according to the method the fitness is defined. It is superior to be less than the minimum value achieved for the fitness. Compute the top location of this loop and name it "The best Location", and compute the alternatives allocated to the variables of the top location, and let PF_A be equal to zero. And it can be defined such as (1) for x = 1 to the number of variables (2) for y = 1 to the number of location alternatives and (3) if x = best location (P_y)means

$$PF_{A_{x,y}} = 0 \quad (18)$$

The probability of choosing alternatives $A_{pbty}(y_{(y=1\ to\ P_y)})$computed with $x_{(x=1 to NV)}$ from the following relationship,

$$A_{pbty} = \frac{PF_{A_{xy}}}{\sum_{y=1}^{P_y} PF_{A_{xy}}} \quad (19)$$

Allocate A_{pbty} equal to PP then all alternatives chosen for all variables of the best location and dedicate rest of the probability to the other alternatives based on the relationship such as (1) for x = 1 to the number of variables (2) for y = 1 to the number of location alternatives and (3) if x = best location (P_y)means

$$A_{pbty} = (1 - PP)\, A_{pbty} \quad (20)$$

Compute the subsequently step locations according to the probabilities assigned to each alternative and replicate above steps as many times as the Loops Number. The search space dimension is modified by inertia weight and it is used to update the search space of location for a dolphin.

$$\begin{aligned}\pi_y(t+1) &= \kappa_t\, \pi_y(t) + \xi_1[C_1(P_{Best} - P_y(t))] \\ &+ \xi_2[C_2(G_{Best} - P_y(t))]\end{aligned} \quad (21)$$

where κ_t is the inertia function and ξ_1, ξ_2 are search speed, it is always constant. The large inertia weight of initial condition is linearly decreased to a small value.

$$\kappa_t = [\kappa(0) - \kappa(\max_i)]\frac{\max_i - t}{\max_i} + \kappa(\max_i) \quad (22)$$

where $\max_i$ is the maximum number of iterations for which the algorithm is executed, $\kappa(0)$ is the initial inertia weight, $\kappa(\max_i)$is the final inertia weight and finally update P_{Best} and based on the new value of fitness function and the new fitness values are $\{Z(y_{new}), P_{Best}, G_{Best}\}$.

$$Z(y_{new}) = fitness(P_{y_{new}}) \quad (23)$$

$$P_{Best} = Z(y_{new}) \quad (24)$$

$$G_{Best} = \min(P_{Best}) \quad (25)$$

To repeat the equations from (13) to (25) until we get the best trust values and the required trust is represented by

$$f_3 = G_{Best} \tag{26}$$

The fitness value of each particle or sensor node can be calculated using (7), (12) and (26) i.e.

$$fitness = \alpha_1 f_1 + \alpha_2 f_2 + \alpha_3 f_3 \tag{27}$$

Where α_1 and α_2 be any constant value between 0 and 1 and $\alpha_3 = 1 - \alpha_1 - \alpha_2$. The new velocity and positions are updated each iteration using (3) and (4) respectively.

Proposed Clustering Model with Multi-Path Distance Vector Routing Protocol

The proposed trusted clustering model can be combined with the standard AOMDV as the base routing protocol. Any mobile node in the network can measure the trust for every neighbor and select the reliable way to transmit data stream. Ad Hoc on-demand Multipath Distance Vector Routing (AOMDV) is basically multipath extensions on top of AODV [27]. It consists of two phases i.e., route discovery phase and route maintenance phase. The route discovery process has been modified to enable multiple paths. They stress on link disjointness of multiple paths so that the paths may share nodes but no edges. Also the loop freedom property of paths is guaranteed by using sequence numbers of nodes. After mentioning link disjointness with a high importance, the authors prefer to use one path at a time rather than simultaneous usage of multiple paths. Their reason to choose single path at a time is the requirement of addressing issues, splitting traffic along each path and packet reordering at the destination. And as a different aspect of AOMDV than AODV, the usage of periodic HELLO messages to detect stale paths can be mentioned. The path trust is a sender who desires to transmit data stream to any receiver; it needs to discover a routing path and assess its credibility. It is calculated according to the reliability of each node on this path. The rationale is that as soon as any node is untrustworthy, the entire path is untrustworthy. Due to the asymmetry of 'trust', the path trust can be divided into two types, the forward path trust and the reverse path trust.

Source to destination trust,

$$= \begin{cases} FWD = \min\{DM_{IFT_{xy}}\} & s \le x \le d-1, y = x+1 \\ REV = \min\{DM_{IFT_{yx}}\} & s \le x \le d-1, y = x+1 \end{cases} \tag{28}$$

where v_s is the sender, v_d is the receiver, v_x and v_y are any two adjacent nodes on the candidate routing path, and the direction of this nodes $v_x \to v_y$ denotes that v_x is the next hop of v_y. In our routing protocol, the secure aware routing path is selected from standard routing attributes such as next and last hop details, hop count, forward path trust (FRT) and reverse path trust (RPT) with calculated fitness values (from section 3.2.3) and the same attributes are used to update the table is shown in table 1.

Table 1 Routing Table for proposed multipath routing

Destination IP address	Destination Sequence number	Advertised Hop count	Path List (1, 2 …)					
			Next hop$_1$	Last hop$_1$	Hop count$_1$	FPT$_1$	RPT$_1$	Fitness$_1$
			.	.	.	.	.	.
			Next hop $_n$	Last hop $_n$	Hop count $_n$	FPT $_n$	RPT $_n$	Fitness $_n$

Route Discovery Phase: Like AODV, when a traffic source needs a route discovery process by generating RREQs. Two fields, namely reverse path trust (RPT) and required trust (RT), are added into RREQ packet. Since the RREQs are flooded network-wide, a node may receive several copies of

the same RREQ. All duplicate copies are examined in AOMDV for potential alternate reverse path. But, reverse paths are formed only using those copies that preserve loop-freedom and disjointness among the resulting set of paths to the source. The route discovery phase performs the following steps with an intermediate node v_u receiving an RREQ packet from a neighbor node v_y.

1. To establish a path between two unconnected nodes (v_x and v_y) with the RPT i.e. $RPT_{yu} = DM_{IFT_{yu}}$ this modification is updated in its routing table. When an intermediate node obtains a reverse path via a RREQ copy, it checks whether there is one or more valid forward paths to the destination. If so, node generates a RREP and sends it back to the source along the reverse path; the RREP includes a forward path that was not used in any previous RREPs for this route discovery. The intermediate node does not propagate the RREQ further. Otherwise, the node re-broadcasts the RREQ copy if it has not previously forwarded any other copy of this RREQ and this copy resulted in the formation/updation of a reverse path.
2. Any intermediate node may receive multiple RREQ copies from other intermediate nodes, then go to step 1. If node v_y is not the source, node v_u creates reverse path to the source using the previous node.
3. If node v_u has a valid route to the destination in its routing table, and the routes sequence number is greater than the destination sequence number in the RREQ, node v_u will generate an RREP to node v_y. Otherwise, node v_u modifies the RPT of the RREQ using $\min\left[RPT_{xy}, Trust_{threshold}\right]$ when $DM_{IFT_{yu}}$ is unknown. Then node v_u increases the value of field Hop Count by one and propagates this modified RREQ packet to all neighbors.

Route Maintenance Phase: Route maintenance in AOMDV is a simple extension to AODV route maintenance. A node generates or forwards a RERR for a destination when the last path to the destination breaks. AOMDV also includes an optimization to salvage packets forwarded over failed links by re-forwarding them over different paths. With multiple paths, the possibility of paths becoming stale is more likely. But using very small timeout values to avoid stale paths can limit the benefit of using multiple paths. Moderate settings of timeout values have been used and additionally HELLO messages to proactively remove stale routes have also been utilized. Security services of proposed routing algorithms are affected not only by general attacks that can be passive, active, node compromise and traffic analysis attacks [13] but also by routing attacks.

Routing and data forwarding are important tasks for sensor nodes. Routing protocols have to be energy and memory efficient; but at the same time, they have to be robust against attacks and node failures. There have been many power-efficient routing protocols proposed for WSNs. However, most of them suffer from security vulnerabilities of one sort or another. In the real world, a secure routing protocol should guarantee the integrity, authenticity and availability of messages in the existence of adversaries of arbitrary power. Every authorized receiver should receive all messages proposed for it and should be capable of proving not only the integrity of every message but also the identity of the sender. Some of the routing attacks are discussed in this section such as black hole or packet drop, wormholes, sinkhole, spoofed, altered, or replayed, selective forwarding and HELLO flood attacks.

Black Hole Attack: Black hole attack is a routing layer attack in which data revolve from other node. The transmission of packets on multiple nodes and dropping of packets mostly occurs on routing layer. Routing protocol is targeted by the attack. Black hole attack will cause powerful effect to the performance of mesh networks.

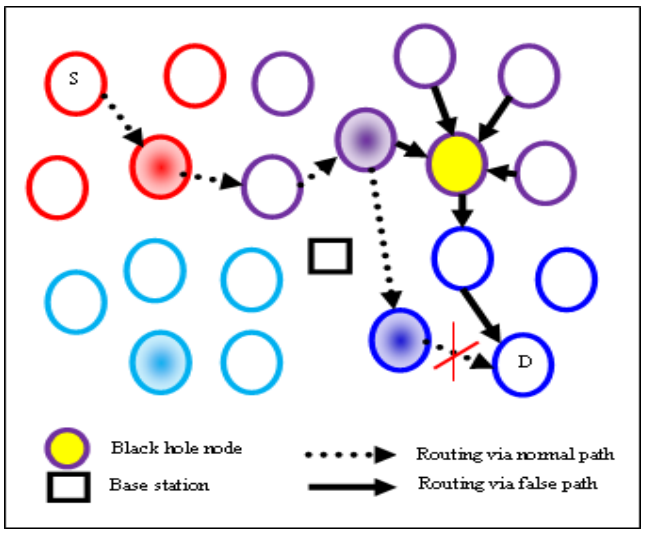

Figure 2. Black Hole attack in WSNs

In black hole attack, the sender node receives reply message from fault node and makes smallest way to receiver node. Fault node sends reply message after authorized node to sender node and then sender become confused in two replies. On that way, Fault node become sender node and the whole data are received by it. In this, the data packets are fully dropped by sender node. The sender node sends a large amount of RREQ messages to every nearby node. When RREQ message is received by fault node, it sends RREP message to sender node, which is non-real and also shows the shortest way to reach to receiver node. Then sender node accepts the reply message from non-real node, which is called fault or black hole node, and transfers the packets. In fig. 2, the black hole node modifies the routing via normal path to attack present path and increase the delay with packet overhead. In the proposed routing, black hole nodes do not

cause serious effects in routing path because every node has an updated trust value with each second and also it is used to frame clustering in WSNs.

Wormhole Attack: Wormhole, in cosmological term, connects two distant points in space via a shortcut route. In the same way in WSNs also one or more attacking node can disrupt routing by short circuiting the network, thereby disrupting the usual flow of packets. If this link becomes the lowest cost path to the destination, then these malicious nodes will always be chosen while sending packets to that destination.

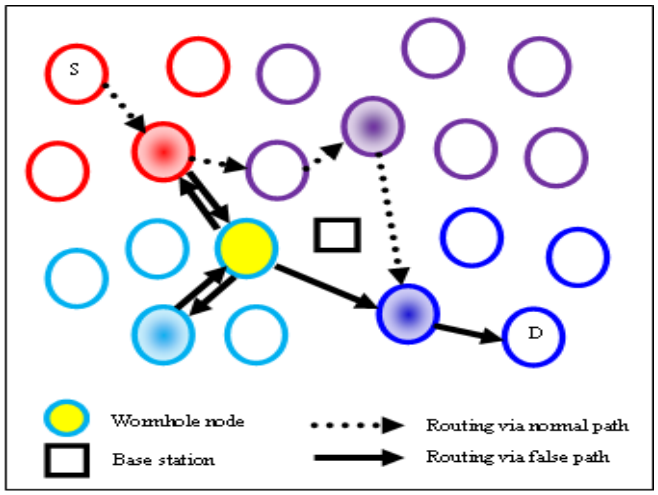

Figure 3. Wormhole attack in WSNs

The attacking node can either monitor the traffic or disrupt the flow. Wormhole attack can be done with single node also but generally two or more malicious nodes connect via a wormhole-link. In fig. 3, the wormhole node modifies the routing by normal path to attack present path. The proposed trusted cluster based routing resists wormhole attack because it is topology hiding and is impossible for attackers to choose central positions to launch the attack and it uses round trip time as a routing metric, which makes it robust against hop count modification.

Sinkhole Attack: By sinkhole attack, the adversary tries to attract nearly all the traffic from a particular area through a compromised node. A compromised node which is placed at the centre of some area creates a large "sphere of influence", attracting all traffic destined for a base station from the sensor nodes.

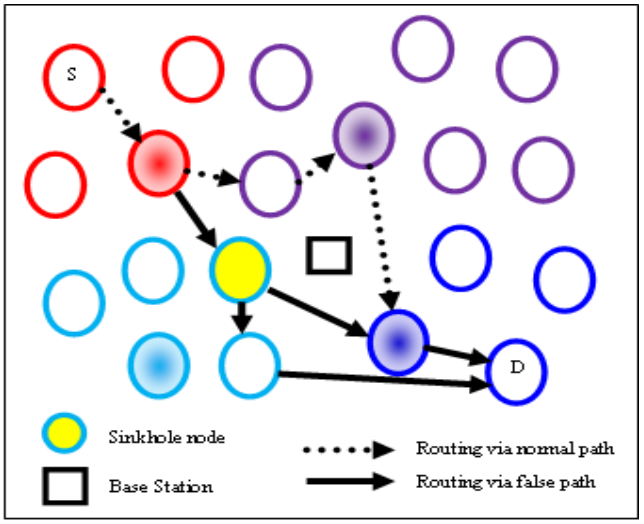

Figure 4. Sinkhole attack in WSNs

The attacker targets a place to create sinkhole where it can attract the most traffic, possibly closer to the base station so that the malicious node could be perceived as a base station. Sinkholes are difficult to defend in protocols that use advertised information such as remaining energy or an estimate of end to end reliability. The proposed trusted cluster based routing resists sinkhole attack because it is impossible for attackers to choose central positions to launch the attack and it uses the node trust value, which makes it robust against base station near nodes.

Spoofing Attack: The most common direct attack targets the routing information exchanged between the nodes. Adversaries may be able to create routing loops, attract or repel network traffic, extend or shorten source routes, generate false error messages, partition the network and increase end to end latency.

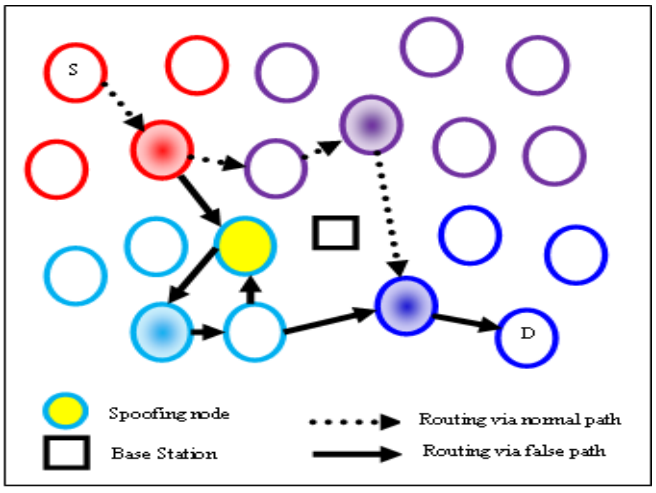

Figure 5. Spoofing attack in WSNs

In fig. 5 show how attack nodes can attract and repeal the network, by advertising a false path and creates a routing loop in the network. The general rule of our proposed protocol is that it does not create the loop in the routing path. From the update of routing attributes in the routing table, the loops are avoided because routing attributes such as hop count, forward and reverse path trust and fitness values of all possible path in the network are considered and these solutions are used to resist spoofing attacks.

Selective Forwarding Attack: In multi hop WSNs, the nodes send packets to the neighboring nodes thinking that they forward messages to destination faithfully. In Selective Forwarding attack, malicious nodes legitimately refuse some packets and drop them. A simple form of this attack is when a malicious node acts like a black hole and drops all the packets passing through it. However, in such an attack, the nodes can detect the attack and can exclude the attacker from routing. A more refined method of this attack is when a malicious node selectively drops or forwards packets.

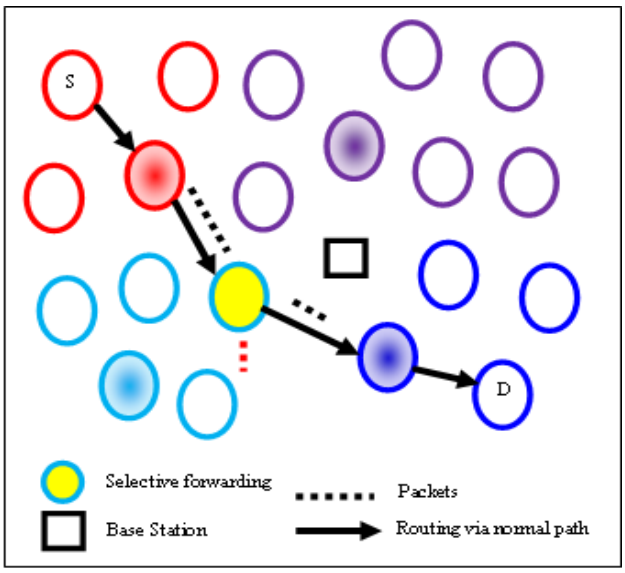

Figure 6. Selective forwarding attack in WSNs

The proposed trust based cluster routing protocol resists selective forwarding attacks by using routing table with trust values, which makes secure routing path. The routing table update process also maintains the packet delivery ratio and packet drop rate of each node and each path.

HELLO Flood Attack: Many protocols require nodes to broadcast HELLO packets for neighbor discovery, and a node receiving such a packet may assume that it is within (normal) radio range of the sender. The result of a HELLO flood is that every node thinks the attacker is within one-hop radio communication range. If the attacker subsequently advertises low-cost routes, nodes will attempt to forward their messages to the attacker. Protocols which depend on localized information exchange between neighboring nodes for topology maintenance or flow control are also subject to this attack. HELLO floods can also be thought of as one-way, broadcast wormholes.

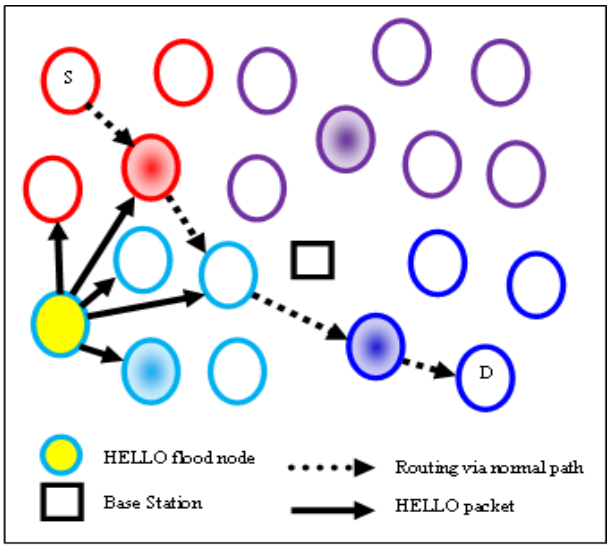

Figure 7. HELLO flooding attack in WSNs

Fig. 7 shows how an attack node broadcasts hello packets to convince nodes in the network and reply the forward packets through it, which renders the energy and data waste. The proposed trusted cluster based routing resist HELLO flood attack because it is impossible for attackers to attack the nearest node due to the trust inference model with trust values.

RESULT AND ANALYSIS

This section discusses lifetime enhanced, energy efficient and secure aware multipath routing scheme for WSNs using Network simulator NS2 tool. The performance metrics such as network life time, delay, energy consumption and packet drop rate of the proposed scheme is compared with RSAP scheme.

Simulation Parameters and Setup

NS-2.34 is adopted to evaluate the performance of proposed protocols in different conditions. Our simulation models a network of 100 to 200 mobile nodes placed randomly within an $1000 \times 1000\,m$ area. Radio propagation range for each node is 250 meters and channel capacity is 2 M bits/sec. Each simulation executes for 180 seconds of simulation time. The IEEE 802.11b Distributed Coordination Function (DCF) is used as the medium access control protocol. A traffic generator is developed to simulate constant bit rate sources. The size of data payload is 1000 bytes. The node mobility uses the random waypoint model. In the following tests, attacks can launch different types of routing attacks, i.e., black hole, wormhole, sinkhole, spoofing, selective forwarding and HELLO flood attacks. To assess the performance of proposed protocols, suitable parameters as given in Table 2 have been

chosen and simulation carried out under various conditions as shown in Table 3.

Table 2. Simulation specification

Parameter	Value
Network size	1000×1000 m
Number of sensor nodes	100-200
Radio propagation range	250 m
Channel capacity	2 M bits/sec
Physical layer	IEEE 802.11b DCF
Data packet size	1000 bytes
Attack types used	black hole, wormhole, sinkhole, spoofing, selective forwarding and HELLO flood
Simulation time	180 Seconds

Table 3. Simulation setup for different test scenarios

Test scenario	Network size	Attack node numbers	Hop counts	Trust threshold	Attack threshold
1	100-200	10	14	0.7	0.4
2	100	5-30	14	0.7	0.4
3	100	10	10-20	0.7	0.4

Scenario 1: Varying network size

In order to evaluate the performance of both the protocols in terms of network life time, end to end delay, energy consumption and packet drop rate, the network size is varied as 100, 120, 140, 160, 180 and 200 with packet size of 1000 bytes.

The main goal of an efficient networking protocol is to enhance the lifespan of the given wireless sensor networks (nodes in general) by minimizing the energy consumption at each node. From the network lifetime versus energy consumption comparison, of different protocols, Fig. 8a shows the results of network life time by varying network size in WSNs and the maximum network life time is in proposed protocol compare to RASP. The proposed protocol improves the network lifetime by 10% compared to the RASP protocol for initial energies of 1 J and 2 J, respectively.

End to end delay is defined as the average time spent in the transmission of data from a source node to sink node on the optimum selected path and most of the latest researches have focused this parameter for quick and on time packet delivery. Here average time delay is considered from sender to sink, which is the combination of maximum delay which can occur during processing, queuing, propagation and retransmission in the network. Fig. 8b shows the results of delay by varying with the network size; the minimum end to end delay is in proposed protocol compared to RASP. The proposed protocol improves the end to end delay by 5% compared to the RASP protocol respectively.

Total energy consumption for the sensor nodes in the given wireless sensor network at different time slots is measured for both the proposed and existing protocol. It is found that with time, there is a gradual increase in the energy consumption of protocol. Fig. 8c shows the results of energy consumption by varying the network size. The energy consumption is very low in the proposed routing protocol compared to RASP. The proposed protocol improves the energy consumption by 10% compared to the RASP protocol respectively.

The topology for this set of experiments consists of approximately 60 nodes, most of which were placed in a line at 0.5m apart. Guided by results from preliminary experiments, some nodes were intentionally removed from near the transmitter and more nodes placed at a finer granularity (0.25m apart) close to the edge of the communication range, giving finer resolution in that region. Our node placement was therefore slightly non-uniform, and it is carefully accounted for this in the analysis. Finally, experiments were conducted carefully over several days to mark node positions so that nodes could be precisely placed. Fig. 8d shows the results of packet drop ratio by varying the network size; the packet drop ratio is very low in the proposed protocol compared to RASP. The proposed protocol reduces the packet loss ratio by 5% compared to the RASP protocol.

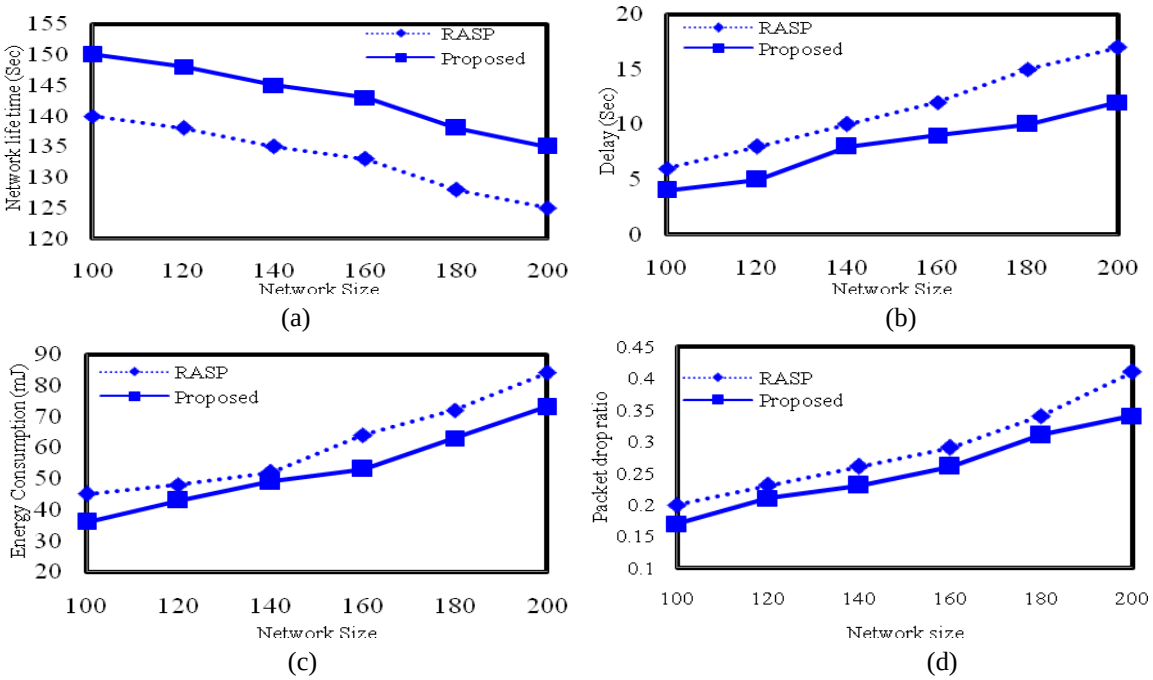

Figure 8. Varying Network size (a) Network life time (b) End to End delay (c) Energy Consumption (d) Packet drop ratio

Scenario 2: Varying number of attack nodes

In order to evaluate the performance of both the protocols in terms of network life time, end to end delay, energy consumption and packet drop rate, the number of attack nodes is varied as 5, 10, 15, 20, 25 and 30 with packet size of 1000 bytes. The attacks are very challenging to prevent. Its success rests on the forwarding node not checking for optimality of the route. Under these circumstances, a loose source routing is defined where the intermediate nodes are replaced by a part or all of the route in the packet header. This makes it necessary for nodes to discover and cache optimal routes to a fraction of other nodes, partially defeating the as-needed discovery advantage. Fig. 9a shows the results of network life time by varying the number of attack nodes in WSNs and the maximum network life time is in proposed protocol compared to RASP. The proposed protocol improves the network lifetime by 8% with attack included in the network compared to the RASP protocol. Fig. 9b shows the results of delay by varying the number of attack nodes; the minimum end to end delay is in proposed protocols compared to RASP. The proposed routing protocol improves the end-to-end delay by 3% with attack included in the network compared to the RASP protocol respectively.

An attack may also be applicable to a recently proposed defense mechanism for hidden services, although it has not been tested. An attack on Tor hidden services exploit the ability to make many requests to a hidden service so that eventually the hidden service connects to a malicious Tor router as the first hop. They recommend using a small set of trusted entry guards as first hops to prevent the attack. However, using essentially the same techniques, a malicious Tor node and hidden service client should be able to recognize when it is the second hop router and obtain very precise estimates of the hidden server's RTT to each of its guard nodes. Fig. 9c shows the results of energy consumption by varying the number of attack nodes; the energy consumption is very low in the proposed routing protocol compared to RASP. The proposed protocol improves the energy consumption by 5% with attack included in the network compared to the RASP protocol.

After sending a massage source node broadcasts a monitor message to all its neighbors instructing them to monitor the action of the next node in the route and start transmitting data. After finishing the transmission, source node sets a time out for the receiving of the postlude message. If source node receives message before the timeout expires and the number of the data packets received by destination is same as the number of data packets sent by source or the data loss is within tolerable range, then source starts the transmission of the next data block. Else it starts the detection and removal of the malicious nodes in the route. Fig. 9d shows the results of packet drop ratio by varying the number of attack nodes; the packet drop ratio is very low in our proposed protocol compared to RASP. The proposed protocol minimizes the loss ratio by 5% with attack included in the network compared to the RASP protocol.

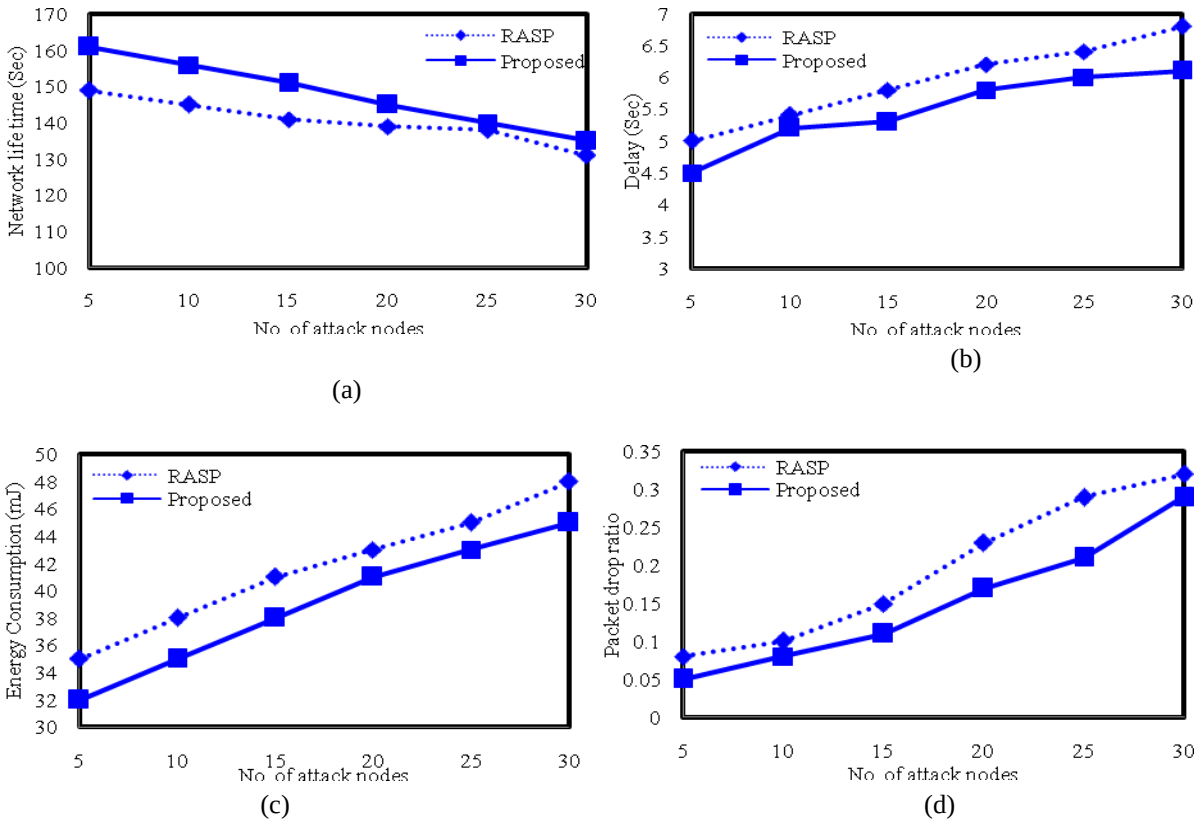

Figure 9. Varying Number of attack nodes (a) Network life time (b) End to End delay (c) Energy Consumption (d) Packet drop ratio

Scenario 3: Varying number of Hop count

In order to evaluate the performance of both the protocols in terms of network life time, end to end delay, energy consumption and packet drop rate, the number of hop count is varied as 10, 12, 14, 16, 18 and 20 with packet size of 1000 bytes. Hop count is probably the most widely used route selection method in a highly dynamic network. Fig. 10 shows the effect of the average number of hops for different network size with different transmission ranges. It shows that the network with less number of nodes has relatively a large average number of hops. It means that as the number of nodes increases, the average number of hops decreases. This characteristic of the network is observed, because in a network to provide connectivity, nodes should be at more distance if they are fewer in number and they should be at less distance if they are larger in number. Fig. 10 also shows that as the hop count increases, the node density of the network also increases.

The hop count per route is time-averaged for source to destination session and is averaged over the entire source to destination sessions of a simulation run. Instead of just taking the average of the entire source to destination paths of source to destination session, the lifetime of these paths is taken into consideration when computing the average hop count. Fig. 10a shows the results of network life time by varying number of hop count in WSNs and the maximum network life time is in proposed protocol compared to RASP. The proposed protocol improves the network lifetime by 15% with increasing number of hop count in the network compared to the RASP protocol. There is an assumption that neighboring nodes are available in the forwarding region and transmission range of source node. A random variable represents the Euclidean distance between the current nodes and the chosen next-hop node according to the criteria of minimum angular deviation. Apparently, min-hop routing algorithm finds the path with the smallest hop count. The proposed routing algorithms often find paths with a very large hop count. Fig. 10b shows the results of delay by varying the number of hop count; the minimum end to end delay is in proposed protocols compared to RASP. The proposed protocol improves the end-to-end delay by 5% with increasing number of hop count in the network compared to the RASP protocol.

The probability of successful transmissions and average effective energy consumption per successfully transmitted packet is described here. It can be seen that, unsurprisingly, the probability of successful transmissions increases from nearly 0 to nearly 1 as the transmission range increases. In contrast, the average effective energy consumption could hardly have been predicted by heuristic reasoning and it needs more explanations. When hop count is small, the network is made of a large number of small components. An increase in hop count will cause an increase in the size of these components. Therefore, the average number of hops for

unsuccessful transmission increases and the energy wasted on unsuccessful transmission also increases. As hop count further increases, although the average number of hops for successful/unsuccessful transmission still increases, the energy wasted on unsuccessful transmission starts to decrease as more source-destination pairs become connected. Fig. 10c shows the results of energy consumption by varying the number of hop counts in WSNs; the energy consumption is very low in the proposed routing protocol compared to RASP. The proposed protocol improves the energy consumption by 4% with increasing number of hop count in the network compared to the RASP protocol.

Minimizing the hop-count maximizes the distance traveled by each hop, which is likely to minimize signal strength and maximize the loss ratio. Even if the best route is a minimum hop-count route, in a dense network there may be many routes of the same minimum length, with widely varying qualities; the arbitrary choice made by most minimum hop count metrics is not likely to select the best. Fig. 10d shows the results of packet drop ratio by varying the number of attack nodes; the packet drop ratio is very low in our proposed protocol compared to RASP. The proposed protocol reduces the loss ratio by 5% with increasing number of hop count in the network compared to the RASP protocol. The performance metrics such as network life time, end to end delay, energy consumption and packet drop ratio of the proposed scheme is compared with RSAP scheme in Table 4.

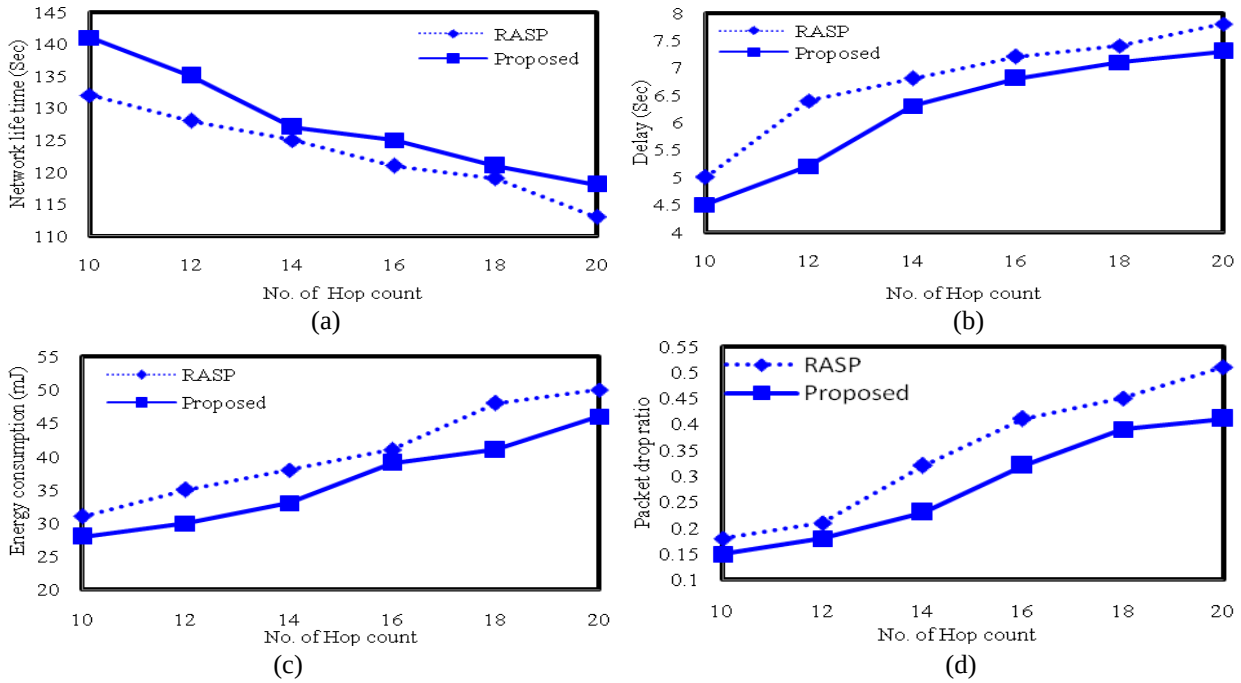

Figure 10. Varying Number of attack nodes (a) Network life time (b) End to End delay (c) Energy Consumption (d) Packet drop ratio

Table 4: Analysis of ranges proposed method and existing methods in terms of different Parameters

Scenarios	Network life time(sec)		End to end delay(sec)		Energy consumption (mJ)		Packet drop ratio	
	Proposed	RASP	Proposed	RASP	Proposed	RASP	Proposed	RASP
Varying network size[100-200]	150-136	140-125	3-10	6-17	35-70	45-85	0.15-0.35	0.2-0.4
Varying no. of attack nodes[5-30]	160-145	150-140	4.5-6	5-6.8	32-44	35-48	0.05-0.25	0.1-0.3
Varying no. of hop count[10-20]	140-120	132-112	4.5-7	5-7.5	27-45	30-50	0.15-0.4	0.2-0.5

CONCLUSION

In this paper a life time enhanced energy efficient and secure aware routing protocols are proposed for WSNs. Dolphin echolocation algorithm is used to calculate the trust value for each node in the network and it is used as one of routing attributes in PSO algorithm cluster formation and cluster head selection process. Trusted cluster based routing protocol combined with standard AOMDV protocol contributes to deliver maximum network life time, energy efficiency and security against different attacks and performance over routing features compared to RASP [13]. The security analysis shows that the proposed approach resists malicious attacks such as black hole, wormhole, sinkhole, spoofing, selective forward and HELLO flooding attacks. The performance analysis shows that the proposed protocols provide better life time, end to end delay, energy consumption and packet drop ratio. From the simulation results, the network lifetime of proposed work is increased by 10%, 8%, and 15% than RASP scheme. The delay of proposed work is decreased by 5%, 3%, and 5% than RASP scheme. The energy consumption of proposed work is decreased by 10%, 5%, and 4% than RASP scheme. The delivery ratio of proposed work is decreased by 5%, 5%, and 5% than RASP scheme. The performance analysis shows that the proposed protocol performance is more efficient and secure than the existing RASP scheme.

REFERENCES

[1] I. Akyildiz, Weilian Su, Y. Sankarasubramaniam and E.Cayirci, "*A survey on sensor networks*", IEEE Commun. Mag., vol. 40, no. 8, pp. 102-114, 2002.

[2] Jongsik Jung, Taekeun Park and Cheeha Kim, "*A forwarding scheme for reliable and energy-efficient data delivery in cluster-based sensor networks*", IEEE Communications Letters, vol. 9, no. 2, pp. 112-114, 2005.

[3] Huang Lu, Jie Li and M. Guizani, "*Secure and Efficient Data Transmission for Cluster-Based Wireless Sensor Networks*", IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 3, pp. 750-761, 2014.

[4] M. Arunraja, V. Malathi and E. Sakthivel, "*Distributed Similarity based Clustering and Compressed Forwarding for wireless sensor networks*", ISA Transactions, vol. 59, pp. 180-192, 2015.

[5] B. Xiao, B. Yu and C. Gao, "*CHEMAS: Identify suspect nodes in selective forwarding attacks*", Journal of Parallel and Distributed Computing, vol. 67, no. 11, pp. 1218-1230, 2007.

[6] H. Ammari and S. Das, "*Forwarding via checkpoints: Geographic routing on always-on sensors*", Journal of Parallel and Distributed Computing, vol. 70, no. 7, pp. 719-731, 2010.

[7] S. MA, H. JI and G. YUE, "*An Energy-Aware Geographical Forwarding Protocol Utilizing Adaptive Sleeping in Wireless Sensor Networks*", The Journal of China Universities of Posts and Telecommunications, vol. 13, no. 1, pp. 15-19, 2006.

[8] M. Busse, T. Haenselmann and W. Effelsberg, "*Energy-efficient forwarding in wireless sensor networks*", Pervasive and Mobile Computing, vol. 4, no. 1, pp. 3-32, 2008.

[9] C. Chao, I. Li, C. Yang and J. Li, "*An efficient diversity-driven selective forwarding approach for replicated data queries in wireless sensor networks*", Journal of Systems Architecture, vol. 57, no. 9, pp. 830-839, 2011.

[10] A. Valera, W. Soh and H. Tan, "*Energy-neutral scheduling and forwarding in environmentally-powered wireless sensor networks*", Ad Hoc Networks, vol. 11, no. 3, pp. 1202-1220, 2013.

[11] S. Pino-Povedano, R. Arroyo-Valles and J. Cid-Sueiro, "*Selective forwarding for energy-efficient target tracking in sensor networks*", Signal Processing, vol. 94, pp. 557-569, 2014.

[12] Rongxing Lu, Xiaodong Lin, Haojin Zhu, Xiaohui Liang and Xuemin Shen, "*BECAN: A Bandwidth-Efficient Cooperative Authentication Scheme for Filtering Injected False Data in Wireless Sensor Networks*", IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 1, pp. 32-43, 2012.

[13] S. Annlin Jeba and R. Suresh Kumar, "*Reliable anonymous secure packet forwarding scheme for wireless sensor networks*", Computers & Electrical Engineering, vol. 48, pp. 405-416, 2015.

[14] P. Rao, P. Jana and H. Banka, "*A particle swarm optimization based energy efficient cluster head selection algorithm for wireless sensor networks*", Wireless Netw, 2016.

[15] P. Mohanty and M. Kabat, "*Energy Efficient Reliable Multi-path Data Transmission in WSN for Healthcare Application*", International Journal of Wireless Information Networks, vol. 23, no. 2, pp. 162-172, 2016.

[16] A. Bader, K. Abed-Meraim and M. Alouini, "*An Efficient Multi-Carrier Position-Based Packet Forwarding Protocol for Wireless Sensor Networks*", IEEE Transactions on Wireless Communications, vol. 11, no. 1, pp. 305-315, 2012.

[17] J. Ren, Y. Zhang, K. Zhang and X. Shen, "*Adaptive and Channel-Aware Detection of Selective Forwarding Attacks in Wireless Sensor Networks*", IEEE Transactions on Wireless Communications, vol. 15, no. 5, pp. 3718-3731, 2016.

[18] Y. Zhang, D. Huang, M. Ji and F. Xie, "*The evolution game analysis of clustering for asymmetrical multi-factors in WSNs*", Computers & Electrical Engineering, vol. 39, no. 6, pp. 1746-1757, 2013.

[19] R. Jin, T. Gao, J. Song, J. Zou and L. Wang, "*Passive cluster-based multipath routing protocol for wireless sensor networks*", Wireless Netw, vol. 19, no. 8, pp. 1851-1866, 2013.

[20] T. Du, S. Qu, F. Liu and Q. Wang, "*An energy efficiency semi-static routing algorithm for WSNs*

based on HAC clustering method", Information Fusion, vol. 21, pp. 18-29, 2015.

[21] S. Mahajan, J. Malhotra and S. Sharma, "*An energy balanced QoS based cluster head selection strategy for WSN*", Egyptian Informatics Journal, vol. 15, no. 3, pp. 189-199, 2014.

[22] G. Hacioglu, V. Kand and E. Sesli, "*Multi objective clustering for wireless sensor networks", Expert Systems with Applications*, vol. 59, pp. 86-100, 2016.

[23] S. Sharma and S. Jena, "*Cluster Based Multipath Routing Protocol for Wireless Sensor Networks*", ACM SIGCOMM Computer Communication Review, vol. 45, no. 2, pp. 14-20, 2015.

[24] S. G, R. D'Souza and G. Varaprasad, "*Digital Signature-Based Secure Node Disjoint Multipath Routing Protocol for Wireless Sensor Networks*", IEEE Sensors J., vol. 12, no. 10, pp. 2941-2949, 2012.

[25] A. Liu, Z. Zheng, C. Zhang, Z. Chen and X. Shen, "*Secure and Energy-Efficient Disjoint Multipath Routing for WSNs*", IEEE Trans. Veh. Technol., vol. 61, no. 7, pp. 3255-3265, 2012.

[26] W. Heinzelman, A. Chandrakasan and H. Balakrishnan, "*Energy-efficient communication protocol for wireless microsensor networks*", Proceedings of the 33rd Annual Hawaii International Conference on System Sciences.

[27] M. Radi, B. Dezfouli, K. Bakar and M. Lee, "*Multipath Routing in Wireless Sensor Networks: Survey and Research Challenges*", Sensors, vol. 12, no. 12, pp. 650-685, 2012.

[28] S. Lindsey and C. Raghavendra, "*PEGASIS: Power-Efficient gathering in Sensor Information Systems*", International Conference on Communications, 2001.

[29] Rabiner, W., Chandrakasan, A., Balakrishnan, H., "*Energy-Efficient Communication Protocol for Wireless Microsensor Networks,*" Hawaii International Conference on System Sciences, Maui, HI, pp.10-19, Jan. 2000

[30] I. F. Akyildiz et al., "*Wireless Sensor Networks: A Survey,*" Elsevier Sci. B. V. Comp. Networks, vol. 38, no. 4, Mar. 2002, pp. 393–422.

[31] W. R. Heinzelman, A. P. Chandrakasan, and H. Balakrishnan, "*EnergyEfficient Communication Protocol for Wireless Microsensor Networks,*" Proc. 33rd Hawaii Int'l. Conf. Sys. Sci., Jan. 2000.

[32] F. Farouk, F. Zaki and R. Rizk, "*Multi-level stable and energy-efficient clustering protocol in heterogeneous wireless sensor networks"*, IET Wireless Sensor Systems, vol. 4, no. 4, pp. 159-169, 2014.

[33] S. Chand, S. Singh and B. Kumar, "*Heterogeneous HEED Protocol for Wireless Sensor Networks",* Wireless Pers Commun, vol. 77, no. 3, pp. 2117-2139, 2014.