SCMRP: Secure Cluster Based Multipath Routing Protocol for Wireless Sensor Networks

Suraj Kumar Sharma
NIT, Rourkela, Odisha, India
Email: suraj.atnitrkl@gmail.com

Sanjay Kumar Jena
NIT, Rourkela, Odisha, India
Email: skjena@nitrkl.ac.in

***Abstract*—WSNs are multihop networks, which depend on the intermediate nodes to relay the data packet to the destination. These nodes are equipped with lesser memory, limited battery power, little computation capability, small range of communication and need a secured and efficient routing path to forward the incoming packet. In this paper, we propose a secure cluster based multipath routing protocol (SCMRP). Researchers have proposed clustered sensor networks to increase the efficiency (i.e. increase system throughput, save energy and decrease system delay by data aggregation) and multipath sensor networks to increase the resilience and reliability of the network. The SCMRP is the combination of these two sensor networks; therefore, it provides efficiency as well as reliability and the proper use of cryptographic algorithm provides sufficient security to the sensor network. SCMRP provides security against various attacks like altering the routing information, selective forwarding attack, sinkhole attack, wormhole attack, Sybil attack etc. Further, we have provided a brief analysis to various issues related to key management, orphan nodes, security and energy efficiency.**

***Keywords*—secure routing, wireless sensor networks, multipath, clustering, resilience, security.**

I. Introduction

The growth of microwave devices, wireless communication and microprocessor technologies devised to the small, low power and low cost sensor node. These self-organized sensor nodes form multihop networks, called wireless sensor networks (WSNs). WSNs are very different than Mobile ad hoc networks (MANETs) in terms of architecture, application and resource capacity. So that the protocols which generally used in MANET, we can't apply directly to the WSN. Therefore in the last one decade researchers are continuously working to enhance efficiency and security of wireless sensor networks. Sensor networks have many applications from the field of medical to battle field and from the homeland security to earthquake monitoring.

The most crucial part of the WSNs is the data communication; data should reach to the sink (i.e. base station) early and as it is. Delay in data or manipulated data is useless for the user. So the essential requirement of data communication is the proper routing, till now number of routing protocols are present. These routing protocols are divided into some classes[1] the main class is based on *network structure* and *protocol operation*; *network structure* is again classified into flat, hierarchical and location based and *protocol operation* has negotiation, multipath, query, QoS, and coherent based, all are having its own advantages and disadvantages, but no one deals with the security.

For maintaining integrity, authenticity and confidentially of the sensed data, security mechanism is must. Security also mark equally as efficiency and lifetime of the network, adding security on already implemented protocol is not feasible. Nowadays, a huge number of researchers are working for secured and efficient routing protocols.

Mainly network layer protocol (i.e. routing protocol) suffers from many attacks[7] like; spoofing or altering the route information, selective forwarding, sinkhole attack, Sybil attack, wormhole attack, HELLO flood attack[1] etc. In this paper we have presented a secure cluster based multipath routing protocol (SCMRP), whose main objectives are: (1) To replace the work load from resource less nodes (i.e. sensor nodes) to resource rich node (i.e. base station); (2) To improve the resilience of the network by multipath routing; (3) To overcome the problem of orphan node; (4) To provide point to point as well as end to end security from different network layer attacks; (5) To enhance efficiency and prolong the lifetime of the network. All these objectives have been achieved in this paper; we provide a detail analysis of the protocol to justify.

The rest of the paper is organised as follows. Section II describes related work. Assumption is listed in Section III. Section IV introduces and describes SCMRP and its five phases: neighbor detection and topology construction, pairwise key distribution, cluster formation, data transmission and re-clustering and re-routing. In section V, we does the detail analysis of SCMRP. We concludes the paper in section VI.

II. Related Work

There are a huge number of routing protocols present for sensor networks. First time these routing protocols were presented in an organized way by Al-Karaki and Kamal[1], this survey covered almost all aspect of routing protocol, classification and architecture. But all these basic protocols have been implemented without the security. Karlof et al.[7] describe the attacks on different routing protocols and provide the countermeasures, which is the base of the many research

[1] All these attack comes under active attack. The attacker is also classified as laptop class attacker - mote class attacker and insider attacker - outsider attacker[7]. Most of the outsider attacker can be prevented by link layer security using a *global shared key*, but in the presence of insider attacker or compromised nodes it is ineffective[7].

978-1-4244-9730-0/10/$26.00 ©2010 IEEE

works. SPINS[13] provides the two generalized mechanism; SNEP for confidentiality, authenticity, integrity and freshness of data and second μTESLA for authenticated broadcasting, but with the extra over head of buffering messages prior to key disclosure that increase the latency and generating own key chain for every single communication.

LEACH[4] is the first and very popular concept of clustered routing without any security. SecLEACH[11] provides an efficient solution for secure communication in LEACH with the help of *random key pre-distribution* and μTESLA and overcomes some of the attacks. Again to provide effective solution for secure communication in LEACH, RLEACH[18] has been introduced with improved random key pre-distribution scheme.

Some work has been done in secure hierarchical routing protocol; Tubaishat et al.[16] have described energy efficient hierarchical routing protocol with group key management scheme, but when changing the cluster head all group keys (i.e. inter cluster and intra cluster) have to calculate again, is an overhead associated with this protocol. NHRPA[5] is also an approach towards secure hierarchical routing which provide security under node compromise attack. Quan et al.[14] offer security against exterior adversary and inner compromised nodes by gene and reputation management tools with extra burden of computation and communication.

All the hierarchical routing protocol has been implemented with the efficiency in mind. If once, we leave the issue of security, there are some other issues exist in clustering protocol like; orphan nodes problem and multihop path (from the cluster head to the base station). In this paper we overwhelmed these two problems.

There are many multipath routing protocols[6], [3] exist, which increase resilience and reliability at the expense of increased energy consumption, traffic generation and overhead of maintaining the alternative paths. In this paper, we overcome these problems with security as a main issue.

Some secure multipath routing protocols have also introduced like; Wenjing Lou[9] has proposed a protocol which is capable of finding multiple node-disjoint paths from the each source node to the common sink(i.e. base station). Parno et al.[12] have implemented a protocol to ensure node-to-node message delivery, even if the sensor network is under active attack. INSENS[2] and SEEM[10] both sent the neighbor information to the base station for computing multipath from source to sink, but in INSENS, BS unicasts the multipath table to each associated nodes and SEEM works as a data centric protocol, which floods the query to the network and the node which satisfies the query will send a request for the routing path to the base station. SEEM justifies the security without using any cryptographic mechanism, unlike INSENS uses cryptography for preventing many attacks.

In this paper, we also use the same mechanism, used in INSENS and SEEM but added the concept of clustering.

III. Sensor Network System Assumption

In the wireless sensor network system lifetime, we follow these assumptions. (1) The sensor nodes are randomly deployed in the network. (2) It is the homogeneous system model where all nodes have similar storage, communication and computation capabilities. (3) BS is secured and possesses a high memory, computation and battery power. (4) Every node has a unique ID, a certificate signed by authority (i.e. base station) and a shared key with the base station. (5) All sensor nodes are static in nature. (6) All sensor nodes are symmetrical, that is same frequency has been used to communicate with each other. (7) Every node has the same energy source that is non-chargeable battery. The sensor node dies as its battery exhausts. (8) In the cluster, there should be only one-hop communication between nodes and cluster head. (9) It is not necessary that the distance between cluster heads and the base station is one-hop. (10) Every sensor node's communication range should be constant and predefined.

IV. Secure cluster based multipath routing protocol (SCMRP)

In this section, we introduce and describe the secure cluster based multipath routing protocol (SCMRP). It is a proactive type protocol, in which all the routes are computed before they really needed. When sensor nodes are static in nature, it is preferable to have table driven protocol (proactive protocol) rather than using reactive protocol[1]. Initially at the time of deployment all node possess unique *ID*, a *certificate* (signed by authority i.e. base station), a *unique shared key* (shared with base station) and a *public key* of the base station. The *certificate* is used to authenticate any node at the time of neighbor detection with the *public key* of the base station; *unique shared key* is used to communicate with the base station through the lifetime of the network.

SCMRP mainly consists of five phase; neighbor detection and topology construction, pairwise key distribution, cluster formation, data transmission and re-clustering and re-routing. In the following section we describe each and every phase of the protocol in detail.

A. Neighbor detection and topology construction

According to the assumption, All node contain ID$\{ID_x\}$, certificate$\{CERT_x\}$, unique shared key$\{K_{xbs}\}$ and public key$\{K_{bs}\}$. For detecting the neighbors, the node starts broadcasting and receiving the NBR_DET packet as shown in fig.1, which contains the *ID* and *CERT* of the node with the following format:

$$x \rightarrow * : \texttt{NBR\_DET} \mid ID_x \mid CERT_x \tag{1}$$

Each node who receives the NBR_DET packet will first authenticate the node *ID* by verifying the certificate $\{CERT_x\}$. If the sender node is authenticated, the receiver node will add its *ID* into the *neighbor_list*, otherwise drop the packet. So that unauthorized node cannot take part in the *neighbor detection* phase. After some time when all have completed their broadcasting, they start sending the neighbor information to the BS in following format:

$$\begin{aligned} x \rightarrow BS &: \texttt{NBR\_INFO} \mid ID_x \mid CERT_x \mid E(K_{xbs}, NBR_x) \mid \\ &MAC(K_{xbs}, \texttt{NBR\_INFO} \mid ID_x \mid CERT_x \mid E(K_{xbs}, NBR_x)) \end{aligned} \tag{2}$$

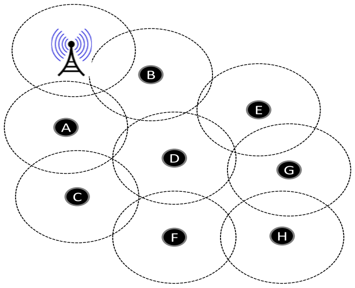

Fig. 1. Node broadcats NBR_DET packet to detect neighbors in the network.

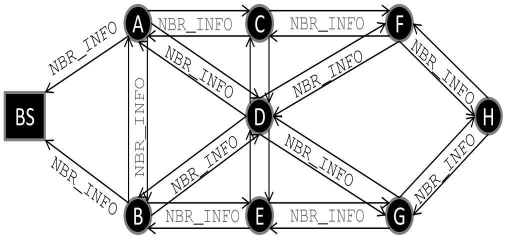

Fig. 2. NBR_INFO packet broadcasts among the network for the base station

Any intermediate node who receive the `NBR_INFO` packet will perform following operations: (1) First check the authenticity of the sender node by its certificate. (2) If the sender node *ID* is authenticated, receiver node rebroadcast the packet. (3) If the receiver node again receives the same packet with same *ID*, simply drops the packet. For that every node maintains a table, called *received_packet* table.

In this way, it reduces the traffic of the network and save some energy of the node. When the `NBR_INFO` packet reaches to the BS as shown in fig.2, BS will verify the MAC for the integrity and authenticity and encrypts the neighbor information with the *unique shared key* between sender node and the base station. We use MAC which is generated by the data and encrypted by the *unique shared key*, so that no adversary can spoof or manipulate the neighbor information.

B. Pairwise key distribution

After getting the neighbor information from all nodes of the network, the base station can visualize the correct topology of the network and produce a *neighbor matrix* by which after applying the DFS algorithm BS can find the multiple path from the BS to every source node. Before that BS has to calculate the secret key for every pair of neighbor nodes, which is called *pairwise key*. The *pairwise key* has been generated by a hash function as follows:

$$K_{xy} = h(secret, ID_x, ID_y)$$

The *secret* which is a random number produced by the base station to generate a *pairwise key*. BS unicasts the pairwise key to the respective nodes with the following format:

$$\begin{aligned} BS \rightarrow x : \texttt{PAIR\_KEY} \mid seq\_no \mid ID_{bs} \mid CERT_{bs} \mid ID_x \mid ID_y \mid \\ E(K_{xbs}, K_{xy} \mid E(K_{ybs}, K_{xy})) \mid \\ MAC(K_{xbs}, \texttt{PAIR\_KEY} \mid seq\_no \mid ID_{bs} \mid CERT_{bs} \mid ID_x \mid \\ ID_y \mid E(K_{xbs}, K_{xy} \mid E(K_{ybs}, K_{xy}))) \end{aligned} \tag{3}$$

The packet format contains *packet_type*, *sequence_no*, *ID* of the BS, its certificate, *ID* of the destination, *ID* of its neighbor, encrypted *pairwise key* for *x* and *y* and MAC of the whole data. Each intermediate node receiving this packet does the following things:(1) First verifies the certificate of the base station with the public key. (2) After that, it checks the *seq_no* and node pair of the packet in the *received_packet* table. If there is no such entry, store the *seq_no*, packet type and pair of node and rebroadcast the packet, otherwise drop it. (3) If the destination node *ID* is same as its own *ID*, encrypt the *pairwise key*, verify the MAC and send the encrypted packet intended for the neighbor node with *nonce* and its own *ID* encrypted with the *pairwise key*, in the following format:

$$x \rightarrow y : \texttt{CHALLENGE} \mid ID_y \mid E(K_{yb}, K_{xy}) \mid E(K_{xy}, ID_x \mid nonce) \tag{4}$$

Node *y* decrypts the packet with the *unique shared key* K_{yb} and gets the *pairwise key*,then decrypts the second packet with the *pairwise key* and sends the following packet back to *x*.

$$y \rightarrow x : \texttt{CHALLENGE\_REP} \mid ID_x \mid E(K_{xy}, ID_y \mid nonce + 1) \tag{5}$$

In this way, both neighbor nodes can verify each other by exchanging the challenge packet and the overhead of again sending the same *pairwise key* to *y* from the base station has been reduced. After the end of this phase every node pair possess a *pairw*ise key. If node *x* does not get back the `CHALLENGE_REP` packet with the expected format, it will send a report to the BS about the fake node, which possesses the *ID* and *certificate* of the legitimate node.

C. Cluster formation

After the *pairwise key* distribution, formation of cluster is initiated by the BS. Election of the *cluster head* is based on the residual energy as explained in EECS[17]. We assume that all node's energy level are same before starting the cluster formation. Now BS will choose 5-8% of the nodes as *cluster head* with the following conditions; (1) no two *cluster heads* will be the neighbor of each other and (2) each *cluster head* possess at least 7-10% of nodes as neighbor. Afterwards BS unicasts the intimation packet (i.e. `CH_INT`) to the *cluster heads* with the calculated *routing path* from the CH to the BS. Let's assume in the intended routing path *node i* is the *next hop*, then the format of `CH_INT` packet is as follows:

$$\begin{aligned} BS \rightarrow CH : \texttt{CH\_INT} \mid ID_{bs} \mid ID_i \mid E(K_{ibs}, PATH \mid seq\_no) \mid \\ MAC(K_{chbs}, \texttt{CH\_INT} \mid ID_{ch} \mid PATH \mid seq\_no) \end{aligned} \tag{6}$$

Each node receiving this packet does the following things: (1) Check the *next hop ID*, if its same as its own, decrypt the PATH and find the *next hop* from the *routing path* (PATH) otherwise drop the packet. (2) Check the *seq_no* in *received_packet* table, if does not exist, then store packet type and *seq_no* and do further changes in the packet, otherwise drop it. (3) Set the *previous hop* as its own *ID* and *next hop* as found in the routing path (PATH). (4) Store the routing table in the memory with *next* and *previous hop* as reverse to forward the data to the BS. (5) Encrypt the PATH and *seq_no* for *next hop* node with the *pairwise key* and broadcast the modified packet.

In this way, when `CH_INT` packet received by CH, It can decrypt the PATH as well as verify the data by MAC and sends an acknowledgement (`ACK`) back to the BS, by following the same *routing path*. After a certain time if BS will not receive any acknowledgement (`ACK`) from the CH, It will again compute the path and resend the `CH_INT` packet. Criteria for computing the *routing path* are: (1) total residual energy of the path and (2) total consumption of the power in the path.

That is the path with greater residual energy and smallest *hop count* has been elected like SEEM[10]. Now for cluster formation the CHs broadcast the `CH_ADV` packet to advertise their will. `CH_ADV` contain the *ID* and *CERT* so that receiver node can verify the authentication. Nodes which receive many advertisements will choose the CH with two criteria: (1) whether the *pairwise key* exist with the advertised *ID* and (2) greater signal strength of the broadcasted advertisement.

After electing the CH, nodes send their will by `CH_JOIN` packet with *ID* and a MAC with the *pairwise key* and a *nonce*. After getting the entire joining request, CH sends the *cluster member* information to the BS and generates a TDMA schedule based on number of member nodes and unicast it to each member. The format of the packets are as follows:

$$CH \rightarrow * : \mathtt{CH\_ADV} \mid ID_{ch} \mid CERT_{ch} \tag{7}$$

$$x \rightarrow CH : \mathtt{CH\_JOIN} \mid ID_x \mid MAC(K_{xch}, \mathtt{CH\_JOIN} \mid ID_x \mid nonce_x) \tag{8}$$

$$CH \rightarrow x : \mathtt{CH\_SHED} \mid ID_x \mid E(K_{xch}, t_x) MAC(\mathtt{CH\_SHED} \mid ID_x \mid E(K_{xch}, t_x) \mid nonce_x + 1) \tag{9}$$

D. Data transmission

This phase mainly consists of three components; first the member node transmits the sensed data to the *cluster head* with the encrypted and authenticated form and can sleep to save energy if does not associated with any route; second the *cluster head* aggregates and compresses the received data to the new signal and sent to the BS with the prescribed route (we consider *node j* is the *next hop* in the routing table); third the BS will use *unique shared key*(with CH) to decrypt and authenticate received data. Let's observe these three components with the following packet formats:

$$x \rightarrow CH : \mathtt{DATA} \mid ID_x \mid E(K_{xch}, d_x) \mid MAC(K_{xch}, \mathtt{DATA} \mid ID_x \mid E(K_{xch}, d_x)) \tag{10}$$

After getting the data, CH aggregates and sends it to BS.

$$CH \rightarrow BS : \mathtt{AGGR\_DATA} \mid ID_{ch} \mid ID_j \mid E(K_{jch}, seq\_no) \mid E(K_{chbs}, d_{ch}) \mid MAC(K_{chbs}, \mathtt{AGGR\_DATA} \mid seq\_no \mid E(K_{chbs}, d_{ch})) \tag{11}$$

Here `AGGR_DATA` is the packet type, ID_{ch} is the *previous hop* and ID_j is the *next hop* of the route, the encrypted *seq_no* is used to check the replying of the packet, if any node receives the `AGGR_DATA` packet with the same *seq_no*, it simply drops the packet. Next is encrypted data (i.e. d_{ch}) for the BS and the MAC for maintaining the integrity and authenticity of the packet. Each node receives this packet perform following operations: (1) Check the *next hop ID*, if it is same as its own *ID*, decrypt the *seq_no*. (2) Check in the *received_packet* table for the packet *seq_no*, if entry is not there then enter the packet type and *seq_no*, otherwise drop it. (3) Change the *next hop* entry with *next hop* node *ID* and the *previous hop* with its own *ID*. (4) Encrypt the *seq_no* with the *pairwise key* of *next hop* and rebroadcast it.

In this way, the data will reach to the BS with the prescribed route and BS will use *unique shared key* (K_{chbs}) to validate the effectiveness of the data.

E. Re-clustering and Re-routing

As mentioned, the selection of CH is based on the residual energy of the node. BS continuously monitors the residual energy of the existing CH, if found below the threshold value it elect another CH based on residual energy and conditions, described earlier. After electing CH, network follows the same procedure to intimate the CH and formation of cluster, as described earlier. The computation of threshold value should depends upon the application.

Likewise if the routing path residual energy goes below the threshold or any node fails, BS selects another path and sends the *routing path* (PATH) to the respective CH. In this way multipath gives resiliency and reliability to the network.

In sensor nodes we use the battery which has limited power[2]. If we assume node energy is 100W and the power for transmitting or receiving one packet is 10 mW, then total number of packets a node can transmit or receive is (100W/10mW) 1000. BS will reduce the total by one each time when a node transmits or receives a packet, and computes the residual energy of the node.

V. SCMRP ANALYSIS

In this section we analysis and observe each and every aspect of SCMRP. First we see the issue behind the key management, new node and orphan node. Then we do the security and energy-efficiency analysis.

A. Issues behind the key management

INSENS[2] used the *global key* for secure neighbor detection, but If the *global key* is compromised whole network get compromised. We use a digitally singed certificate $CERT_i$ (i.e. issued by the BS to every node). So that, no adversary can create a forge *ID*.We recommend to use improved rabin's digital signature scheme[8] which consumes very less computation cost for verification.

[2] We observe AA batteries with different material like NiMH, which gives 70 W (250 kJ), nickel-cadmium having 40-60 W and 100-160 W of energy for Li-ion.

Instead of *ID*, *certificate* and a *public key* each node has a *unique shared key* with the base station. Any node who wants to send a message to the base station will encrypt it and create a MAC with the *unique shared key*, so that only BS can access it. So that, any adversary can't perform eavesdropping or altering to the message.

Every node trusts on BS, which works as a secured trusted party and distributes the *pairwise key* to nodes with the *unique shared key*. The *pairwise key* distribution works just like Kerberos[15]. Before actually using the *pairwise key* both nodes can authenticate each other by the Kerberos mechanism. In this way if any fake node using the *ID* and *certificate* of other node, will not be able to use *pairwise key*. By this, the *Sybil* attack can be prevented.

B. Pairwise key Establishment with a new node

When any *new node* introduces in the network it want to be the part of the communication network. *New node* will broadcast the `NEW_JOIN` in the following format:

$$new \rightarrow * : \texttt{NEW\_JOIN} \mid ID_{new} \mid CERT_{new} \qquad (12)$$

Each neighbor, who receives the `NEW_JOIN` packet, does the following things:

- Check the authenticity of the node by verifies the certificate ($CERT_{new}$), if found legitimate, add its *ID* to the *neighbor_list*.
- Send the information to the BS about the *newly joined node* with the packet format (2) and wait for the *pairwise key*.
- After getting the *pairwise key* and an encrypted packet intended to *new node*, the *neighbor node* sent a `CHALLENGE` to the *new node* with the packet format (4) and wait for the `CHALLENGE_REP`.

The *pairwise key* establishes, as soon as the *neighbor node* get back the `CHALLENGE_REP` with the expected format.

C. The orphan nodes problem

Almost all clustering protocols are suffering from the *orphan nodes* problem. The node which does not belong to any cluster called the *orphan nodes*[11]. The node become orphan by many reasons; like doesn't possess the *pairwise key* or *shared key* or out of range. In SCMRP, at the time of clustering, when CHs broadcast the advertisement, it does not reach to the node which is not in the range. The *orphan nodes* generally have the neighbors but no CH. In fig.3, *node O* will become the *orphan node*, if BS elects *node G* and *node D* as CHs. There are some solutions for *orphan nodes* exist like; allow them to sleep till it doesn't get any CH request, add a small protocol that would allow the already adopted children to bring the *orphan nodes* into their clusters or let them to communicate directly with the BS[11].

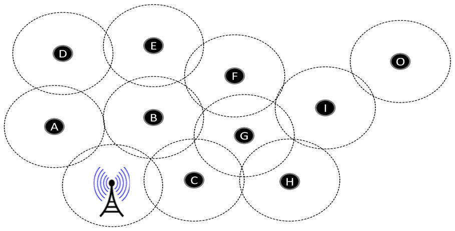

Fig. 3. Orphan node (node O when node G and D elected as CHs)

However, SCMRP is able to deal with the *orphan nodes* by allowing them to send a *route request* to the BS with the following format:

$$orphan \rightarrow BS : \texttt{RREQ} \mid ID_{orp} \mid seq\_no \mid CERT_{orp} \mid$$
$$MAC(K_{orpbs} \mid \texttt{RREQ} \mid seq\_no \mid ID_{orp} \mid CERT_{orp}) \qquad (13)$$

After getting the *route request*(RREQ), BS sent the *route reply*(RREP) by computing the *routing path*, with the following format:

$$BS \rightarrow orphan : \texttt{RREQ} \mid ID_{bs} \mid ID_i \mid E(K_{ib}, PATH \mid seq\_no) \mid$$
$$MAC(K_{orpbs}, \texttt{RREQ} \mid ID_{orp} \mid PATH \mid seq\_no) \quad (14)$$

In this way, routing path reaches to the *orphan node* and it can send the sensed data to the base station, till it doesn't get any clustering request from the CHs. This approach is very advantageous in the application where each and every sensor node's data is precious. The increment of *orphan node* may decrease the performance of the network. In this case, we have to restrict the number of *orphan node* requests.

D. Security against different attacks

Karlof et al.[7] summarize various attacks against the routing protocol. In the following , we discuss each of them and show how the proposed protocol prevents those attacks.

***Sybil attack*:** In the SCMRP a malicious node can possess multiple identities[3], but does not able to own the *unique shared key*. At the time of *pairwise key* establishment our protocol checks the authenticity of the neighbor node and send the report to the BS if any discrepancy happens. So the BS removes that node from the *neighbor_list* of the legitimate node and modifies the network topology.

***Sink hole and Wormhole attack*:** *Sinkhole* attack mainly works by making a compromised node look attractive to the neighbor nodes to route the data packet and generally spoof, modify or drop the packet. In this way, *sinkhole* attack give birth to many attacks like; *selective forwarding*, *blackhole*, *tempering the routing information* etc. An adversary launch *wormhole* with two distant malicious nodes and try to attract the traffic by showing one hop distance to the sink. *Wormhole* attack is very difficult to detect because it uses out-of-bound channel to route packets[7].

However, in the SCMRP the *routing paths* are computed and maintained by the BS. Therefore, whatever an adversary performs, it has no impact on the selection process of *routing path*.

***Selective forwarding attack*:** SCMRP does not allow any

[3] Because, at the time of neighbor detection every node broadcast their *ID* and *certificate*.

malicious node to join the routing path, because BS decides the *routing path* and distribute it to the respective node in the secured manner, so no adversary can alter it. Along with this, we use a *seq_no* associated with every data packet; if it drops by the malicious node, it will be detected by the *next hop* node and it sends a report to the BS and it selects another *routing path*.

HELLO flood attack**:** SCMRP is also subjected to this attack, because it needs the *neighbor information* to create *routing path*. Initially our assumption was, all nodes should be homogeneous in nature so a mote class attacker cannot increase its transmission range and in this paper we are not dealing with laptop class attacker. Anyhow, if *HELLO flood* attack happens to the network, the adversary has to prove its authentication to BS; to be the part of the network and to launch an attack, which is not possible without the *unique shared key*. Just broadcasting the overheard packet is not enough to affect the network.

Spoofing or altering the route information**:** An adversary can launch the routing information corruption by spoofing, altering or replying the routing information. By this an adversary can attracts or redirects the traffic, increases the latency, generate routing loops or creates false error[7] etc.

However, SCMRP uses *pairwise key* as well as *unique shared key* to distribute the routing information, so it is very difficult for an adversary to launch *routing information corruption* attack.

E. Energy-efficiency analysis:

SCMRP used the concept of multipath as well as clustering. It is a hybrid approach to deal with security and efficiency. BS is responsible for calculating the multipath as mentioned in SEEM[10] and INSENS[2]. Nasser and Chen found that, SEEM increases the network lifetime about 35% as compared to Directed Diffusion[6].

Secondly, SCMRP used clustering approach based on residual energy as mentioned in EECS[17], which also increase the network lifetime 35% over LEACH[4]. Besides of theses facts some features are there like; Instead of nodes, BS calculates routing path , cluster heads and pairwise key to the nodes; BS maintains the network topology; Kerberos mechanism reduces (almost half) the traffic of the network; CHs also lessen the degree of data traffic of the network. So that, we can say our proposed protocol is energy efficient and is able to enhance network lifetime.

VI. Conclusion

In data communication the most crucial part is to aggregate the data and route it to the reliable and secure path. In this paper, we have described the secure and reliable routing protocol, which collects the neighbor's information of the nodes at the base station, computes *pairwise key* and energy efficient multipath for each node, helps make the clusters by selecting the CHs. CHs aggregate the data and route it to the BS. BS is continuously monitoring the nodes for residual energy to select some new paths and CHs. SCMRP is designed based on using cluster and multipath concepts and provides following advantages: (1) security towards various network layer protocol attacks; (2) efficiency and reliability to the network; (3) eliminated the problem of orphan node; (4) resiliency to the path on node failure; (5) alleviate the burden of the sensor node by transferring route and key related task to the base station.

References

[1] J. N. Al-karaki and A. E. Kamal. Routing techniques in wireless sensor networks: A survey. *IEEE Wireless Communications*, 11(6):6–28, December 2004.

[2] J. Deng, R. Han, and S. Mishra. Insens: Intrusion-tolerant routing in wireless sensor networks. *Computer Communications In Dependable Wireless Sensor Networks*, 29(2):216–230, January 2006.

[3] D. Ganesan, R. Govindan, S. Shenker, and D. Estrin. Highly-resilient, energy-ecient multipath routing in wireless sensor networks. *ACM SIGMOBILE Mobile Computing and Communications Review*, 5(4):11–25, 2001.

[4] W. Heinzelman, A. Chandrakasan, , and H. Balakrishnan. Energy-efficient communication protocols for wireless microsensor networks. In *Proc. 33rd IEEE Hawaii International Conference on System Sciences*, volume vol.8, pages 4–7, January 2000.

[5] C. Hong-bing, Y. Geng, and H. Su-jun. Nhrpa: a novel hierarchical routing protocol algorithm for wireless sensor networks. *The Journal of China Universities of Posts and Telecommunications*, 15(3):75–81, September 2008.

[6] C. Intanagonwiwat, R. Govindan, and D. Estrin. Directed diffusion: a scalable and robust communication paradigm for sensor networks. In *Proc. the 6th annual international conference on Mobile computing and networking (MobiCom'00)*, pages 56–67. ACM, 2000.

[7] C. Karlof and D. Wagner. Secure routing in sensor networks: Attacks and countermeasures. *Ad Hoc Networks*, 1:293–315, May 2003.

[8] K. Kurosawa and W. Ogata. Efficient rabin-type digital signature scheme. *Designs, Codes and Cryptography*, 16(1):53–64, January 1999.

[9] Wenjing Lou. An efficient n-to-1 multipath routing protocol in wireless sensor networks. In *In: Proc. 2nd IEEE International Conference MASS*, pages 665–672, Washington D.C., November 2005.

[10] N. Nasser and Y. Chen. Seem: Secure and energy-efficient multipath routing protocol for wireless sensor networks. *Computer Communications*, 20(11-12):2401–2412, 2007.

[11] L. B. Oliveira, A. Ferreira, M. A. Vilaa, H. C. Wong, M. Bern, R. Dahab, and A. A. F. Loureiro. Secleach-on the security of clustered sensor networks. *Signal Processing*, 87(12):2882–2895, December 2007.

[12] B. Parno, M. Luk, E. Gaustad, and A. Perrig. Secure sensor network routing: a clean-slate approach. In *Proc. the 2006 ACM CoNEXT conference*, pages 1–13, Lisboa, Portugal, December 2006. ACM.

[13] A. Perrig, R. Szewczyk, J.D. Tygar, V. Wen, and D. E. Culler. Spins: Security protocols for sensor networks. *Wireless Networks*, 8(5):521–534, September 2002.

[14] Z. Quan and J. Li. Secure routing protocol cluster-gene-based for wireless sensor networks. In *Proc. The 1st International Conference on Information Science and Engineering (ICISE2009)*, pages 4098–4102, December 2009.

[15] J. G. Steiner, G. Neuman, and J. I. Schiller. Kerberos: An authentication service for open network systems. In *Proc. the Usenix Winter Conference, Berkeley*, pages 191–202, February 1988.

[16] M. Tubaishat, J. Yin, B. Panja, and S. Madria. A secure hierarchical model for sensor network. *ACM SIGMOD Record*, 33(1):7–13, March 2004.

[17] M. Ye, C. Li, G. Chen, and J. Wu. Eecs: An energy efficient clustering scheme in wireless sensor networks. In *Proc. of the IEEE International Performance Computing and Communications Conference*, pages 535–540. IEEE Press, 2005.

[18] K. Zhang, C. Wang, and C. Wang. A secure routing protocol for cluster-based wireless sensor networks using group key management. In *Proc. 4th IEEE International conference on Wireless Communications, Networking and Mobile Computing (WiCOM'08)*, pages 1–5, October 2008.