ISSN No. 0976-5697

Volume 2, No. 3, May-June 2011

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Secure Routing Based on ECC in Cluster Wireless Sensor Networks

Rayala Upendar Rao*, Madarapu Naresh Kumar
Department of Computer Science
Pondicherry University, INDIA
{rayalaupendar, madarapu.naresh } @gmail.com

K Palanivel
Systems Analyst, Computer Centre,
Pondicherry University, INDIA
kpalani@yahoo.com

Abstract: wireless sensors having limited capabilities, because of these factors sensors possess huge attacks like sinkhole, worm hole, Sybil, flooding, etc. a lot of research work already done, but no one implemented secure routing protocol to mitigate all these attacks. Some proposals came on security of wireless sensor network which controlled only one or two attacks. We proposed Secure Routing in Cluster based Wireless Sensor Networks (SRECWSN) with access control mechanism, which has developed on Elliptic Curve Cryptography. Cluster topology is suitable for low power devices like sensors and provides efficient secure routing. Compare to RSA, Elliptic Curve Cryptography gives great security and it takes less memory.

Keywords: wireless Sensor Networks, Access Control, Cluster Routing, Secure routing.

I. INTRODUCTION

Wireless Senor Network (WSN) is an emerging technology that can be deployed in such a situation where human interaction is not possible like border area tracking enemy moment or fire detection system [5]. The processing capabilities in sensor nodes are generally not as powerful as those in the nodes of wired networks. Complex cryptographic algorithms consequently are impractical for WSNs. Most WSNs are deployed in remote or hostile environments where nodes are disclosed to physical attacks. This is because anyone can access the deployment area and these sensors lack tamper-resistance property [7].

Along with the explosive growth of computer networks in the last decades, the security of information transmitted over the networks has become an ever-increasing concern among the network users. It is well known that there are various attacks that threaten the confidentiality, integrity and availability of the information [4]. Current routing protocols optimize for the limited capabilities of the nodes and application specific nature of the networks, but they are not considering security [9].

More specifically, sensor nodes will do local processing to reduce communications and consequently energy costs. We believe that most efficient and adaptive routing model for WSN is cluster based hierarchical model. In cluster based sensor network, the cluster formation plays a key factor to the cost reduction, where cost refers to the expense of setup and maintenance of the sensor networks. After deployment, any two cluster heads are assumed to be able to communicate directly. A sensor node is only required to communicate with the nearest cluster head. It is assumed that these communications can all be done directly (no intermediate nodes required). It is not assumed that cluster heads are tamperproof, and therefore there is the possibility that cluster heads might be compromised. The attack model is the standard "node capture" model. Our main focus is on routing security in wireless sensor networks.

In rest of the paper discussed as follows. In section II, we have given related work (existing work). In section III, we focus on analysis of different types of attacks in wsn. In section IV, we explore our proposed secure routing model in clustered based wsn. In rest of paper, we discussed comparative results, conclusion, references in section V, VI, and VII respectively.

II. RELATED WORKS

The proposed sensor network routing protocols are highly susceptible to attacks. Adversaries can attract or repel traffic flows, increase latency, or disable the entire network with some times as little effort as sending a single packet. In this section, we survey the proposed sensor network routing protocols and highlight the relevant attacks.

A. TinyOS beaconing

The TinyOS beaconing protocol constructs a breadth first spanning tree rooted at a base station. The base station broadcasts a route update at regular interval. All nodes receiving the update mark the base station as its parent and rebroadcast the update. The algorithm continues recursively with each node marking its parent as the first node from which it hears a routing update during the current time. All packets received or generated by a node are forwarded to its parent (until they reach the base station).

Attacks: The TinyOS beaconing protocol is highly vulnerable to attack. Since routing updates are not authenticated, it is possible for any node act as a base station and become the destination of all traffic in the network.

B. Directed Diffusion

Directed diffusion [11] is a data-centric routing algorithm for describing information out of a sensor network.

Base stations flood interests for named data, setting up gradients within the network designed to draw events (i.e., data matching the interest). Nodes able to satisfy the interest disseminate information along the reverse path of interest propagation. Nodes receiving the same interest from multiple neighbouring nodes may propagate events along the corresponding multiple links. Interests initially specify a low rate of data flow, but once a base station starts receiving events it will reinforce one (or more) neighbour in order to request higher data rate events. This process continues recursively until it reaches the nodes generating the events, causing them to generate events at a higher data rate. Alternatively, paths may be negatively reinforced as well. There is a multipath variant of directed diffusion [12] as well.

Attacks: Due to the robust nature of flooding, it may be difficult for an adversary to prevent interests from reaching targets able to satisfy them.

C. Geographic Routing

Geographic and Energy Aware Routing (GEAR) [2] and Greedy Perimeter Stateless Routing (GPSR) [3] leverage nodes positions and explicit geographic packet destinations to efficiently propagate queries and route replies. GPSR uses greedy forwarding at each hop, routing each packet to the neighbour closest to the destination. When holes are encountered where greedy forwarding is impossible, GPSR recovers by routing around the perimeter of the void. One drawback of GPSR is that packets along a single flow will always use the same nodes for the routing of each packet, leading to uneven energy consumption. GEAR attempts to remedy this problem by weighting the choice of the next hop by both remaining energy and distance from the target.

Attacks: Location information misrepresentation, Sybil attack.

D. Minimum Cost Forwarding

Minimum cost forwarding [10] is an algorithm for efficiently forwarding packets from sensor nodes to a base station with the useful property that it does not require nodes to maintain explicit path information or even unique node identifiers. It works by constructing a cost field starting at the base station. The base station has cost zero. Every other node maintains the minimum cost required to reach the base station. Cost can represent any application dependent metric: hop count, energy, latency, loss, etc.

Attacks: sinkhole attacks, HELLO flood attack, a laptop - class adversary can disable the entire network by transmitting an advertisement with cost zero powerful enough to be received by every node in the network.

E. LEACH:

Low-Energy Adaptive Clustering Hierarchy LEACH [13] renders clustering to efficiently disseminate queries and gather sensor readings to and from all nodes in the network. LEACH assumes every node can directly reach a base station by transmitting with sufficiently high power. LEACH organizes nodes into clusters with one node from each cluster serving as a cluster-head. Nodes first send sensor readings to their cluster-head, and the cluster-head aggregates or compresses the data from all its "children" for transmission to a base station.

Attacks: HELLO flood attack, selective forwarding attack, Sybil attack.

F. Rumor Routing

Rumor routing [14] is a probabilistic protocol for matching inquiries with data events. However, flooding can be used to create a network-wide gradient field [10], which is useful in routing frequent or numerous events or queries and amortizes the initial setup cost. In rumor routing, when a source observes an event, it sends an agent on a random walk through the network. When an agent arrives at a new node, it informs that node of events it knows of (and the next hop on the path to those events), adds to its event list any events the node might know of, and decrements it's TTL. If the TTL is greater than zero, the node probabilistically chooses the agent's next hop from its own neighbours minus the previously seen nodes listed in the agent. When a base station wants to disseminate a query, it creates an agent that propagates in a similar way. A route from a base station to a source is established when a query agent arrives at a node previously traversed by a event agent that satisfies the query.

Attacks: The denial-of-service attack, flooding attack.

G. *Dynamic En-Route Filtering Scheme for false reports*

This scheme [15] is working on Diffie-Hellman key algorithm. In that they loaded the keys in pre-node deployment phase for security purpose. After deploying sensors, start their function of sensing information from physical environment and forwarding data in regular intervals or when base station request for information. After some time sensors exhaust their power or sensors will get repaired. So to replace these nodes, new node deployment phase is necessary. But proposed scheme applicable for only fixed size networks, they are not discussed about new node deployment which creates a bad life time of sensor network.
Attacks: Sybil attack, wormhole attack, sinkhole attack.

III. ANALYSES OF DIFFERENT ATTACKS in WSN

Many sensor network routing protocols are quite simple, and for this reason are sometimes even more susceptible to attacks against general ad-hoc routing protocols. Most network layer attacks against sensor networks fall into one of the following categories:

- Spoofed, altered, or replayed routing information
- Selective forwarding
- Sinkhole attacks
- Sybil attacks
- Wormholes
- HELLO flood attacks
- Acknowledgement spoofing

A. Spoofed, altered, or replayed routing information

The most direct attack against a routing protocol is to target the routing data exchanged between nodes. By spoofing, altering, or replaying routing information,

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, increase end-to-end latency, etc [4].

B. Selective Forwarding

In a selective forwarding attack, malicious nodes may refuse to forward certain messages and simply drop them, ascertaining that they are not propagated any further. A simple form of this attack is when a malicious node behaves like a black hole and refuses to forward every packet she sees [5].

C. Sinkhole Attacks

In a sinkhole attack [1, 4], the adversary's goal is to lure nearly all the traffic from a particular area through a compromised node, creating a metaphorical sinkhole with the opponent at the centre. Because nodes on, or near, the path that packets follow have many opportunities to fiddle with application data, sinkhole attacks can enable many other attacks (selective forwarding, for example). Sinkhole attacks typically work by making a compromised node look especially attractive to surrounding nodes with respect to the routing algorithm. For instance, an adversary could spoof or replay an advertisement for an enormously high quality route to a base.

D. Sybil Attack

In a Sybil attack [1], a single node presents multiple individualities to other nodes in the network. The Sybil attack can significantly reduce the potency of fault-tolerant schemes such as distributed storage, disparity and multipath routing, and topology maintenance [8]. Replicas, storage partitions, or routes believed to be using disjoint nodes could in actuality be using a single adversary presenting multiple identities. Sybil attacks also pose a significantly threat to geographic routing protocols.

E. Wormhole Attack

In the wormhole attack [1][6], an adversary tunnels messages received in one part of the network over a low latency link and replays them in a different part. The simplest instance of this attack is a single node situated between two other nodes forwarding messages between the two of them. However, wormhole attacks more commonly involve two distant malicious nodes colluding to understate their distance from each other by relaying packets along an out-of-bound channel available only to the attacker [4].

F. HELLO Flood Attack

Many protocols require nodes to broadcast HELLO packets to announce themselves to their neighbours, and a node receiving such a packet may assume that it is within (normal) radio range of the sender. This assumption may be false. An attacker with a high powered antenna can convince every node in the network that it is their neighbour. If the attacker also advertises a high quality route it can get every node to forward data to it. Nodes at a large distance from the attacker will be sending their messages into oblivion leaving the network in a state of confusion. This attack can also be thought of as a type of broadcast wormhole. Routing protocols dependant on localized information is extremely vulnerable to such attacks [4].

G. Acknowledgement Spoofing

Various sensor network routing algorithms rely on implicit or explicit link layer acknowledgements. Due to the constitutional broadcast medium, an adversary can spoof [9] link layer acknowledgments for "overheard" packets addressed to neighbouring nodes. Goals include convincing the sender that a weak link is strong or that a dead or disabled node is alive. For example, a routing protocol may select the next hop in a path using link reliability. Artificially reinforcing a weak or dead line is a subtle way of manipulating such a scheme. Since packets sent along weak or dead links are lost, an adversary can effectively mount a selective forwarding attack using acknowledgement spoofing by encouraging the target node to transmit packets on those links.

IV. PROPOSED SCHEME: SRECWSN

The routing protocols discussed above don't provide any security features against attackers. So the main goal is to ensure the secure routing of data in cluster based wireless sensor networks. To provide secure routing, it is needed to concentrate on both routing as well as security to the routing misbehaviour, depending from flooding attacks etc.

A. *Architecture for Secure Routing based on ECC in Cluster based Wireless Sensor Network (SRECRWSN)*

Proposed Architecture contains four modules. Three are horizontal modules and one is vertical module, which works on remaining three horizontal modules. Before using the network deployment of nodes should do in pre-deployment module, here the nodes should be loaded with digital certificate contains both node identity and geographic location assigned by certification authority and store the bootstrapping times, defined as the time taken to load itself to connect the network. Afterwards we need to do the formation of clusters and routing of sensing information. Here we are using intra cluster routing algorithm is discussed above. Finally in new node deployment there is a possibility for malicious nodes entry, so to avoid this we are using access control mechanism on ECC. It ensures security parameters like authentication, integrity and confidentiality.

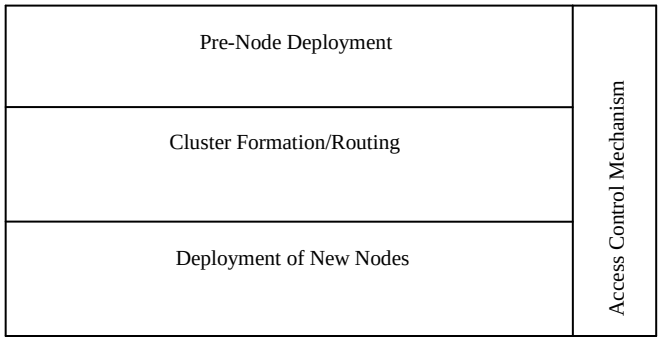

Figure1. Architecture for SRECWSN

B. Access Control Mechanism

Transfer the sensing information in confidential manner from nodes to the target node (base station) by using encryption methods. Even though there is possibility to

divert the packets to other routes or specific node to drain out the limited energy. Nodes in sensor network may be lost due to power exhaustion or malicious attacks. To extend the life time of sensor network, deployment of new nodes is necessary. To prevent malicious nodes from joining the sensor network, access control is required in the design of sensor network protocols. So in this situation we need to control the access rights of the sensor nodes. By using access control mechanism is able achieve authentication, integration and confidentiality. There by we can mitigate the attackers from spoofing, routing misbehaviour and unauthorized access. We propose an access control protocol based on Elliptic Curve Cryptography (ECC) for sensor networks. Our access control mechanism includes not only identity like conventional methods but also takes bootstrap time into consideration.

To provide the security we have to consider the two important factors, authentication and key establishing. ECC provides two popular algorithms they are, Elliptic Curve Digital Signature Algorithm (ECDSA) and Elliptic Curve Diffie-Hellman key algorithm. Each algorithm provides authentication and key establishing respectively. Usually access control mechanism needed in following scenarios, when handshaking of old node and new node, which will be discussed in new node deployment module and another scenario between two old nodes,

We should consider the following parameters have given by certification authority (CA). F_q is a finite field over prime number, let E should be elliptic curve then prime field over curve represented as $E(F_q)$, G points generator of curve, n is the order of curve, T is bootstrapping time. Let N_i, N_j are two nodes, s_i is private key of node N_i then calculate public key as follows. Qi= si*G where G is generator function. Node N_i calculates signature according to elliptic curve digital signature algorithm. Generated signature is pair indicated as (l_i, m_i). To convert binary sequence into integers Hash algorithm is needed. Node N_i is intended to send the message m to N_j. k is a random variable selected from integers.

a) *Authentication Mechanism (ECDSA)*

The following steps indicates signature generation algorithm.

1. Calculate e = HASH (m), where HASH is a Cryptographic hash function, such as SHA-1
2. Select a random integer k from [1,n − 1]
3. Calculate $l_i = x_i \pmod n$, where $(x_i, y_i) = k * G$. If $l_i = 0$, go to step 2
4. Calculate $m_i = k^{-1}(e + s_i l_i) \pmod n$. If $m_i = 0$, go to step 2
5. The signature is the pair (l_i, m_i)

If node Ni sends message to N_j, to authenticate N_i, N_j should know the public key of N_i. The following procedure will explain about signature verification algorithm.

1. Verify that r and s are integers in [1,n − 1]. If not, the signature is invalid.
2. Calculate e = HASH (m), where HASH is the Same function used in the signature generation.
3. Calculate $w = s^{-1} \pmod n$
4. Calculate $u_1 = ew \pmod n$ and $u_2 = l_i w \pmod n$
5. Calculate $(x_i, y_i) = u_1 G + u_2 Q_A$
6. The signature is valid if $x_i = l_i \pmod n$, invalid

Otherwise

b) key sharing mechanism (ECDH)

ECDH ensures secrete key between two parties by using their public data and private data. Third party does not know the private data by using any public data of node. Before establishing the shared key both parties should agree on domain parameters. Node can generate public key as Q=s*G. let (s_i, Q_i) be the pair of the private key-public key of node Ni and (s_j,Q_j) be the pair of private key-public key of node N_j. the following steps explains algorithm for key establishing between two parties.

1. The end node N_i computes $K = (x_K, y_K) = si * Qi$
2. The end node N_j computes $L = (x_L, y_L) = sj * Qj$
3. Since $si*Q_i = s_i*s_j*G = s_j*s_i*G = s_j*Q_j$. Therefore $K = L$ and hence $x_K = x_L$
4. Hence the shared secret is x_K

By integrating these two algorithms (ECDSA&ECDH) into routing transmits the data in secure manner via authentication and key sharing mechanism.

C. Pre-Node Deployment

Before going to utilize the sensor network deploy the nodes manually. Deployment of nodes may be one time activity or continues process. If installation of nodes one time activity, then life time of network will expire in certain period of time. To extend the life time of sensor network, deployment of sensors should be continues process. This continues deployment will extends not only network life time but also extend the network. Placing of sensors categorized into two types, they are random manner and fixed manner.

After deployment of wireless sensors, they have to load with parameters assigned by certification authority (CA) given above. Unlike traditional routing algorithms not only consider the identity of node (digital certificate which contains both node identity and geographic location of the node given by access control mechanism) but also it considers bootstrapping time further security. Access control mechanism can be used in two scenarios, when one handshake happens between two new nodes (initial horizontal module- pre-node deployment) and another handshake happens between old node and new node (which will happens in new node deployment).

a) Handshake between New Nodes.

This scenario will have to consider only after deployment of sensors (in pre-node deployment). We assume that all sensors nodes will maintain same bootstrapping times with tolerable values. Let t is the current time maintained by the legitimate nodes. If they will take loading time T after completion length of the bootstrapping time, present node time is determined as |T+t|. Let we consider two nodes N_i, N_j digital certificate C asserted by certification authority (CA). Each node checks neighbour node identity and the nodes shares shared keys by using Diffie-Hellman key algorithm. Here we consider one more parameter bootstrapping time for more security. Authentication process as follows, one

node checks identity of digital certificate (consist of node location and identity) and bootstrapping time.

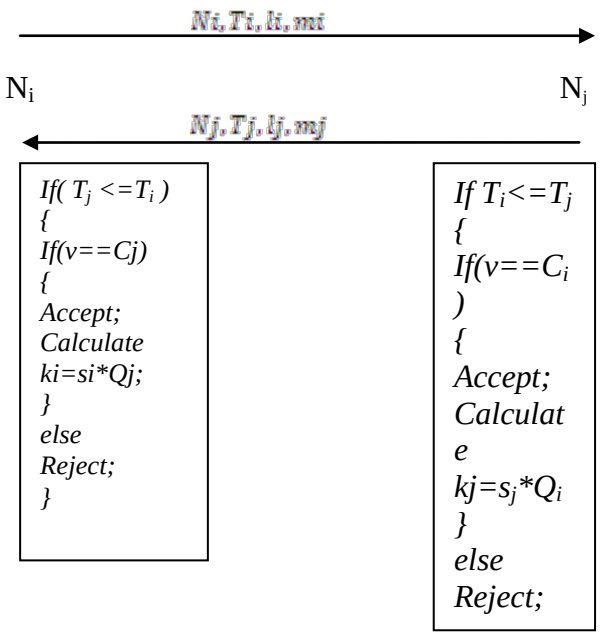

Figure2. handshake between two new nodes, both nodes should authenticate eachother.

D. Dynamic Energy Distribution Cluster Routing

This is the second horizontal module ensures cluster formation and routing. To integrate routing algorithm with access control mechanism, hence we proposed a Dynamic Energy Distribution Cluster Routing (DEDCR). It is very efficient algorithm in cluster based wireless sensor networks. This algorithm supports scalability, energy efficient and adaptive routing. The role of cluster head need to change after some time, why because CH takes the responsibility of forwarding sensing information from node itself and other cluster nodes. So energy of CH will drain out shortly. To remove this drawback we introduced DEDCR. It consists of three phases. They are,

- Cluster head selection
- Cluster formation
- Cluster routing

a) Phase 1: Cluster head selection

Cluster head selection phase starts and all deployment nodes send their energy levels to the base station (BS). We assume that the nodes deployed in different regions, so each region identified by unique id and they will send their nodes information to the base station. Each region will get the particular time slot to send their topological information. Here there is a possibility to occur collision. For example more than one region willing to send their topological information, it could be handled by MAC resolution protocol. After sending information of particular region to base station, the base station verifies nodes identity and selects cluster head based on energy level node. The base station unicast the information to node selected as CH. See the fig3.

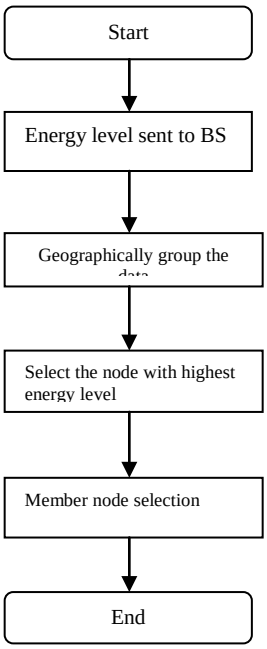

Figure.3 CH selection

b) Phase 2: Cluster Formation

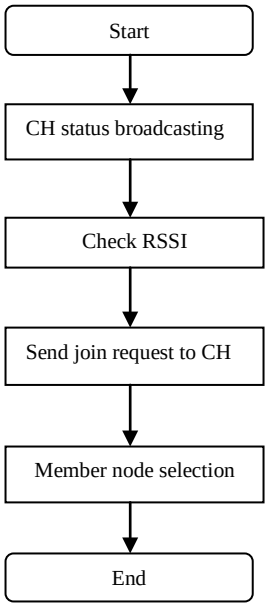

Figure4. Cluster formation

After receiving the unicast information from base station and there is a chance to deploy malicious node, will act as base station. To avoid this harmful action node uses ECDSA and the node should broadcasts its status as Cluster Head to all nodes in that particular region. Those nodes will get high Receive Signal Strength Indicator (RSSI) value; they are willing to join this cluster. The node sends join request to the respective cluster head and in response to join, verifies

nodes identity and confirmed alert is sent by the cluster head. In this way clusters are formed with one cluster head each. Figure4 shows flow diagram of cluster formation phase.

c) Phase3: Intra Cluster Routing

Original Intra cluster routing as the routing phase starts the nodes first check their location if their location is inside the close region then the mode of routing for these nodes is direct routing and on the other hand if the nodes are out of close region their mode of routing is multi-hop. For more information see the figure5.

Direct hop routing : it is possible when node maintains the link with destination node. The topology of this routing is like mesh network. In this each node maintains direct link with all nodes. so this type of network will take more cost and very effiecient.

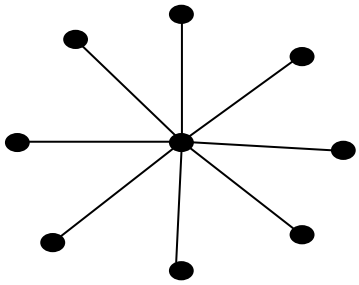

Figure6. Direct hop routing

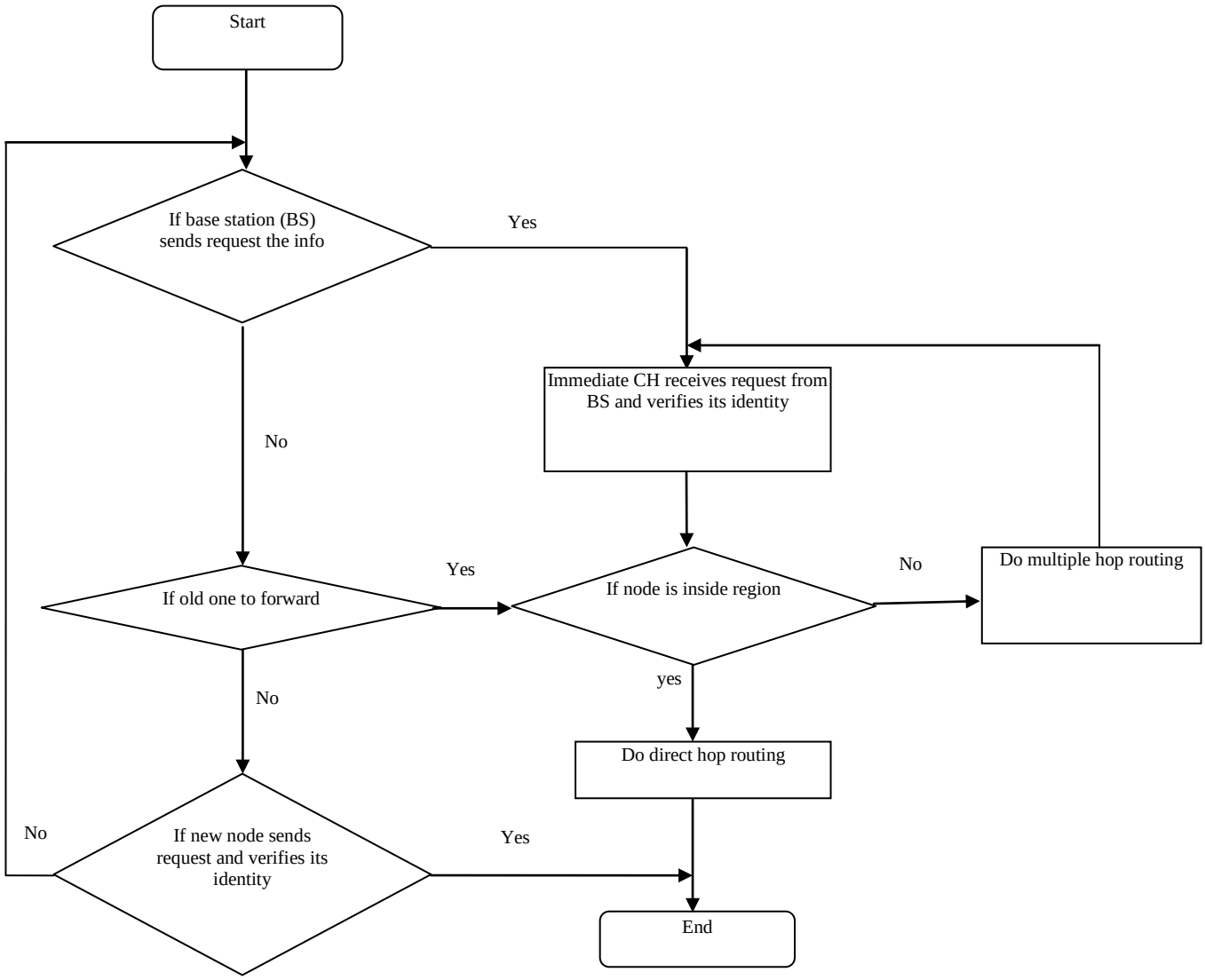

Figure.5. Intra cluster Routing

Multi hop routing: direct routing is not applicable in all applications. For example if node is far from destination node, then it needs to take several intermediate nodes to reach the destination. So the intermediate nodes should have the nature of farwarding.

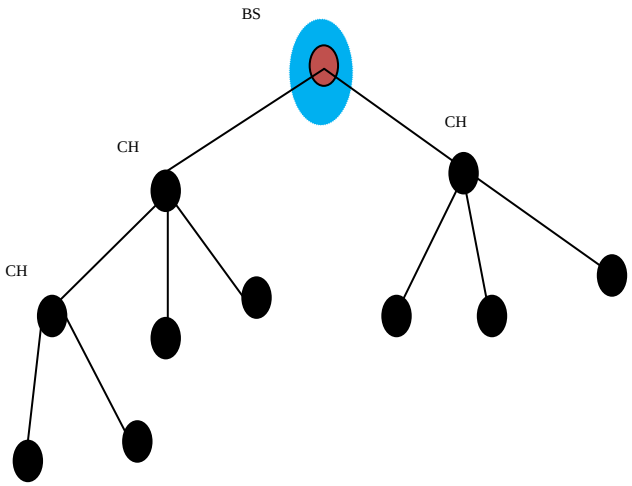

Figure7. Multi hop routing

The distance between source and destination measured in terms of hop count. If the hop count between source node (sender) and destination node is more than two we can go for select multi hop routing, otherwise direct routing will take more time to reach the destination. The hop cost depends on the link between the nodes. All nodes should not maintain same hop costs (links), it depends on the sensors capacity and environmental factors.

E. New Node Deployment

It is last module in proposed architecture. Deployment of nodes may be one time activity or continues process. To extend the life time of network deployment of sensor nodes should be continues, so new deployment module is needed to install new nodes with existing nodes. It is useful for not only for extend the network length but also to replace nodes those will get repair.

New node deployment will give the way for attackers to deploy the malicious nodes. The attacker act as new node act as legitimate one. To mitigate the actions of attackers we have to use the authentication mechanism. Here the communication will be taking in between old node and new node. The old should authenticate new node by verifying its identity and if the signature is valid it will checks the bootstrapping time of the new node. If it satisfies the tolerate value of bootstrapping time then old node allows to connect with network. Otherwise if it is not satisfy both conditions, old node simply discards the new node request.

Consider below scenario (figure.8) for more information. Let the new node identity N_i and the old node identity N_j. The new node will have to generate the public key and private key that should be lies in range of prime field. Here the old node (neighbour node in network which is nearer) should follow the ECDSA to authenticate the identity of old node. The new node will generate the signature by using public key and private key. The node generates public key, by multiplying random generator number with private key.

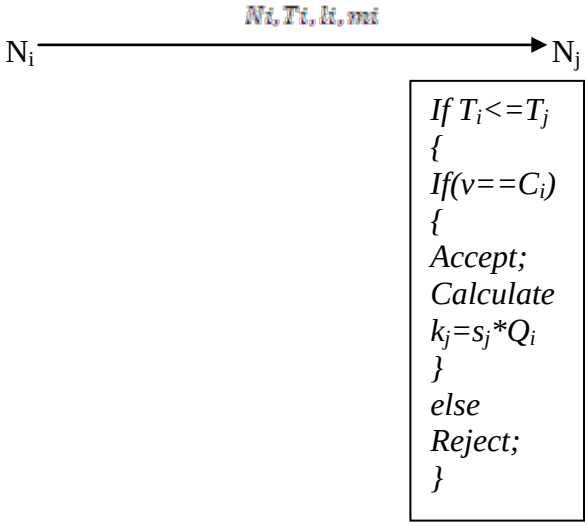

Figure8. shows handshake between two old node and new nodes,

V. COMPARITIVE RESULTS

We compare access control mechanism on elliptic curve cryptography with popular RSA algorithm. ECC is giving more security compare to RSA, which is taking fewer bits key and providing more security. ECC is seen to be the standard for the next generation cryptographic technology. The reason is that ECC can achieve the same level of security with smaller key sizes. It has been shown that 160-bit ECC provides comparable security to 1024-bit RSA and 224-bit ECC provides comparable security to 2048-bit RSA. Under the same security level, smaller key sizes of ECC offer merits of faster computational efficiency, as well as memory, energy and bandwidth savings.

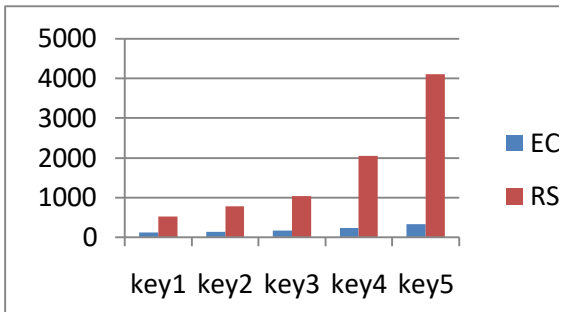

Figure.9 Comparison of security parameter with different key size's of ECC with RSA

Here x- axis represents the key number and y- axis represents key size

VI. CONCLUSION

In this paper, we design and implemented secure routing in cluster based wireless sensor networks, it has access control mechanism developed on ECC. We concentrated on both routing as well as well as security. ECC is better suited

for the resource constrained devices. Due to the merits of ECC, our access control protocol uses 160-bit ECC as the underlying cryptographic infrastructure. Particularly, the signature operation in our protocol is based on the Elliptic Curve Digital Signature Algorithm (ECDSA) which provides authentication mechanism, and the shared key is established according to the Diffie–Hellman algorithm over ECDLP which provides secrete key sharing for secure transmission.

VII. REFERENCES

[1]. Hemanta Kumar Kalita, Avijit Kar, "*Wireless Sensor Network Security Analysis*," International Journal of Next-Generation Networks (IJNGN), Vol.1, No.1, December 2009,1-9.

[2]. Yan Yu, Ramesh Govindan, Deborah Estrin, "*Geographical and Energy Aware Routing: a recursive data dissemination protocol for wireless sensor networks*," Aug 2001.

[3]. Brad Karp, H. T. Kung, "*GPSR: Greedy Perimeter Stateless Routing for Wireless Networks*," MobiCom 2000.

[4]. Pooja Sharma, Pawan Bhadana, "*An Effective Approach for Providing Anonymity in Wireless sensor Network: Detecting Attacks and Security Measures*," (IJCSE) International Journal on Computer Science and Engineering Vol. 02, No. 05, 2010, 1830-1835.

[5]. Shivangi Raman, Amar Prakash, Kishore Babu Pulla, Prateek Srivastava, Ashish Srivastava, Shveta Singh, "*Wireless sensor networks: A Survey of Intrusions and their Explored Remedies*," International Journal of Engineering Science and Technology Vol. 2(5), 2010, 962-969.

[6]. Zaw Tun and Aung Htein Maw, "*Wormhole Attack Detection in Wireless Sensor Networks*," world Academy of Science, Engineering and Technology 46 2008,545-550.

[7]. Yun Zhou, Yanchao Zhang, Yuguang Fang, "*Access control in wireless sensor networks*," Ad Hoc Networks 5 (2007) 3–13.

[8]. Jiang Du, Su Peng, "*Choice of Secure Routing Protocol for Applications in Wireless Sensor Networks*," 2009 International Conference on Multimedia Information Networking and Security.

[9]. Chris Karlof and David Wagner, "*Secure Routing in Wireless Sensor Networks: Attacks and countermeasures*," Ad Hoc Networks 1 (2003) 293–315.

[10]. Fan Ye, Alvin Chen, Songwu Lu, Lixia Zhang, "*A Scalable Solution to Minimum Cost Forwarding in Large Sensor Networks*," in Tenth International Conference on Computer Communications and Networks, 2001, pp. 304–309.

[11]. C. Intanagonwiwat, R. Govindan, and D. Estrin, "*Directed diffusion: A scalable and robust communication paradigm for sensor networks*," in Proceedings of the Sixth Annual International Conference on Mobile Computing and Networks (MobiCOM '00), August 2000, 58-67.

[12]. D. Ganesan, R. Govindan, S. Shenker, and D. Estrin, "*Highly-resilient, energy-efficient multipath routing in wireless sensor networks*," Mobile Computing and Communications Review, oct 2001, Volume 1, Number 2,1-13.

[13]. Wendi Rabiner Heinzelman, Anantha Chandrakasan, and Hari Balakrishnan,"*Energy-Efficient Communication Protocol for Wireless Micro sensor Networks*," Proceedings of the 33rd Hawaii International Conference on System Sciences – 2000.

[14]. D. Braginsky and D. Estrin, "*Rumour routing algorithm for sensor networks*," in First ACM International Workshop on Wireless Sensor Networks and Applications, 2002.

[15]. Zhen Yu, Member, IEEE, and Yong Guan, Member, IEEE, "*A Dynamic En-route Filtering Scheme for Data Reporting in Wireless Sensor Networks*," IEEE/ACM Transactions On Networking, Vol. 18, No. 1, February 2010,150-163.

