www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 6 Issue 4 April 2017, Page No. 20859-20867
Index Copernicus value (2015): 58.10 DOI: 10.18535/ijecs/v6i4.10

ECIES for Group Key Establishment in WSN for Secure Multicast Communication

Miss.P.Prasanna Laxmi[1], Mrs. M.Anupama[2]
[1]M.Tech 2nd Year Student, Department of CSE, MVSREngg College,
Nadergul, Hyderabad, Telengana-501510, India
prasanna.pasham@gmail.com
[2]Assoc. Professor, Department of CSE, MVSR Engg College,
Nadergul, Hyderabad, Telengana-501510, India
anu_meduri@yahoo.co.in

Abstract:*A wireless sensor network (WSN) as the name suggest is a wireless network with spatially distributed autonomous devices making use of sensors for monitoring physical or environmental conditions. WSNs find applications in areas like healthcare, home automation, traffic control etc. WSN with characteristics of self-organization, multi-hop, dynamic topology and limited energy resources, make it extremely difficult to prolong the lifetime of the network. To prolong the life time of WSN with limited energy resources, Multicast can better meet the requirements of network resources. It has an active significance for WSN to increase its performance in the near future. In Wireless sensor networks sensor nodes are grouped together by forming multicast groups. The communication among the nodes is done by broadcasting and multicasting efficient message deliveries among resource-constrained sensor nodes. Two group key protocols are developed for secure multicast communications among the resource-constrained devices. The proposed approach compares the performance of two protocols with ten nodes in each group. We analyze the proposed solution to evaluate the performance using Network Simulator-2 (NS-2) under different network parameters with a number of destination nodes.*

Keywords:*ECIES(Elipticcureve integration encrypted schema),*

1. Introduction

A wireless sensor network consists of sensor nodes capable of collecting information from the environment and communicating with each other via wireless transceivers. The collected data will be delivered to one or more sinks, generally via multi-hop communication. The sensor nodes are typically expected to operate with batteries and are often deployed to not-easily-accessible or hostile environment, sometimes in large quantities. It can be difficult or impossible to replace the batteries of the sensor nodes. On the other hand, the sink is typically rich in energy. Since the sensor energy is the most precious resource in the WSN, efficient utilization of the energy to prolong the network lifetime has been the focus of much of the research on the WSN. The communications in the WSN has the many-to-one property in that data from a large number of sensor nodes tend to be concentrated into a few sinks. Since multi-hop routing is generally needed for distant sensor nodes from the sinks to save energy, the nodes near a sink can be burdened with relaying a large amount of traffic from other nodes. Sensor nodes are resource constrained in term of energy, processor and memory and low range communication and bandwidth. Limited battery power is used to operate the sensor nodes and is very difficult to replace or recharge it, when the nodes die. This will affect the network performance. Optimize the communication range and minimize the energy usage, we need to conserve the energy of sensor nodes .Sensor nodes are deployed to gather information and desired that all the nodes works continuously and transmit information as long as possible. Sensor nodes spend their energy during transmitting the data, receiving and relaying packets. Hence, designing routing algorithms that maximize the life time until the first battery expires is an important consideration.

In some applications the network size is larger required scalable architectures. Energy conservation in wireless sensor networks has been the primary objective, but however, this constrain is not the only consideration for efficient working of wireless sensor networks. There are other objectives like scalable architecture, routing and latency. In most of the applications of wireless sensor networks are envisioned to handled critical scenarios where data retrieval time is critical, i.e., delivering information of each individual node as fast as possible to the base station becomes an important issue. It is important to guarantee that information can be successfully received to the base station the first time instead of being retransmitted. In wireless sensor network data gathering and routing are challenging tasks due to their dynamic and unique properties. Many routing protocols are developed, but among those protocols cluster based routing protocols are energy efficient, scalable and prolong the network lifetime .In the event detection environment nodes are idle most of the time and active at the time when the event occur. Sensor nodes periodically send the gather information to the base station. Routing is an important issue in data gathering sensor network, while on the other hand sleep-wake synchronization is the key issues for event detection sensor networks.

A wireless sensor network (WSN) consists of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on.

Wireless Sensor Networks (WSNs) are a key building block. Typically, sensors are considered resource-constrained devices with limited battery power and computation capabilities. Therefore, it is more effective and efficient to convey multicast messages to a group of devices rather than sending energy consuming unicast messages to individual devices in multiple copies. Securing the group key establishment incline to form the key functionality to provide integrity, authentication, and confidentiality for message transmissions in these multicast groups. Besides, group key establishment protocols have to support device and network characteristics in IoT-enabled WSNs such as resource constraints, scalability, and dynamic group formation. The field of applying multicast is as manifold as the application area of IoTitself, including smart homes, smart cities, environmental monitoring, and healthcare.

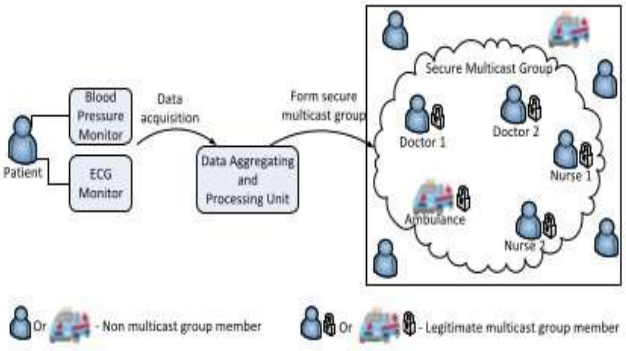

Fig 1.1. Example of use case for multicast group creation for medical application.

In Wireless Sensor Networks it is more effective and efficient to convey multicast messages to a group of devices rather than sending energy consuming unicast messages to individual devices in multiple copies. The admin collects data from source, generates the key and communicates with the destination nodes, which react according to the data acquired, and directs it to the respective multicast group. The multicast groups must be securely formed and respective secret keys have to be shared among all multicast group members to ensure secure communications. The two group key protocols are established for secure multicasting in WSN application paradigms. The two protocols are based on Elliptic Curve Cryptographic operations. These protocols are analyzed on the parameters like overhead, cost and packet delivery ratio.The objective of this protocol is to provide the high level security for the WSN and to form a secure multicast group by establishing group key protocol

2. Literature Survey

The WSN is built of "nodes" from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. Each such sensor network node has typically several parts. A wireless sensor network (WSN) consists of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The development of wireless sensor networks was motivated by military applications and consumer applications, such as industrial process monitoring and control, machine health monitoring. Nodes in these networks utilize same random access wireless channel, cooperating in a friendly manner to engaging themselves in multi hop forwarding. The nodes in the network not only act as hosts but also routers that route to/from other nodes in the network. Because of this dynamic topology the network changes frequently, whenever packets need to be send from source node to destination node the broadcasting mechanism is to be followed as the might be out of range. Within a cell, a base station can reach all mobile nodes without routing via broadcast in common wireless network. In case of ad hoc network each node must be able to forward data for other nodes. This creates additional problems along with problems of dynamic topology which leads to unpredictable connectivity changes.

In fact due to the broadcast nature of the wireless medium, a single packet transmission will lead to multiple receptions. Typically, sensors are considered resource-constrained devices with limited battery power and computation capabilities .Therefore, it is more effective and efficient to convey multicast messages to a group of devices rather than sending energy consuming unicast messages to individual devices in multiple copies. So, the nodes have to cooperate for the integrity of the operation of the network. The process of forwarding the request continues as long as one of the candidate nodes succeeds in receiving and forwarding the packet, the data transmission will not be interrupted. However, nodes may refuse to cooperate by not forwarding packets for others for selfish reasons and not want to exhaust their resources. Various other factors make the task of secure communication in wireless networks difficult include the mobility of the nodes, limited availability of resources, limited processing power. The technology of wireless networks which is dynamic has been deployed in military applications. Commercial interest in such military applications has recently grown due to the advances in wireless communications. [5] In this we study of ad hoc network routing protocols in grid environment and how to form a multicast group among nodes. And it makes the comparison of DSDV and DSR routing protocols, by using performance matrices and average end to end delay, packet delivery fraction, average routing load and data packets lost.

Multicast communication [6] is recommended for constrained IoT networks to reduce the bandwidth usage, and minimize the energy consumption and processing overhead at the terminals. Both multicast and security are key needs in these networks. It presents a method for securing multicast communication in LLNs based on the DTLS security protocol which is already present in CoAP devices. This is achieved by using unicast DTLS-protected communication channel to distribute keying material and security parameters to group members. Group keys consisting of a Traffic Encryption Key (TEK) and a Traffic Authentication Key (TAK) are generated by group members based on the keying material received. A group member uses its DTLS record layer implementation to encrypt a multicast message and provide messageauthentication using the group keys before sending the message via IP multicast to the group.

Although Datagram Transport Layer Security (DTLS) handshake is designed for device-to-device authentication [6], it does not support multicast security. we study a fully implemented two way authentication security scheme for the Internet of Things based on existing Internet standards, especially the [9] Datagram Transport Layer Security (DTLS) protocol. The security scheme is based on the most widely

used public key cryptography (RSA), and works on top of standard low power communication stacks. We believe that by relying on an established standard, existing implementations, engineering techniques and security infrastructure can be reused, which enables easy security uptake. An implemented system architecture for the proposed scheme based on a low-power hardware platform suitable for the IoT. And also a two way authentication is introduced. The authentication is performed during a fully authenticated DTLS handshake and based on an exchange of X.509 certificates containing RSA keys. It provides message integrity, confidentiality and authenticity with affordable energy, end-to-end latency and memory overhead which make it a feasible security solution for the emerging IoT. TESLA [8] scheme which provides a solution to the source authentication problem under the assumption that the sender and receiver are loosely time synchronized. The basic TESLA protocol has the following salient properties. Low computation overhead. On the order of one MAC function computation per packet for both sender and receiver. Periodically, the sender also needs to send out the secret keys. Perfect loss robustness. If a packet arrives in time, the receiver can verify its authenticity eventually (as long as it receives later packets). TESLA is proposed for the broadcast authentication of the source and not for protecting the confidentiality of multicast messages but TESLA is still lacking the compatibility with IoT characteristics. Efficient and Secure Source Authentication for Multicast [12] focuses on substantial modifications and improvements to TESLA. One modification allows receivers to authenticate most packets as soon as they arrive (whereas TESLA requires buffering packets at the receiver side, and provides delayed authentication only). Other modifications improve the scalability of the scheme, reduce the space overhead for multiple instances, increase its resistance to denial-of-service attacks, and more. It reduce the communication overhead when multiple TESLA instances with different authenticationdelays are used concurrently and derive a tight lower bound on the disclosure delay. Ram RatanAhirwal et al,presented Elliptic curve cryptography and Diffie–Hellman key agreement protocol [15], it is an anonymous (non-authenticated) key-agreement protocol, it provides the basis for a variety of authenticated protocols, and is used to provide forward secrecy for web browsers application using HTTPS. Additionally, it provides bidirectional encryption of communications between a client and server, which protects against eavesdropping and tampering with or forging the contents of the communication.

Diffie–Hellman establishes a shared secret that can be used for secret communications by exchanging data over a public network. The key part of the process is that sender and receiver exchange their secret keys in a mix only. Finally this generates an identical key that is mathematically difficult (impossible for modern supercomputers to do in a reasonable amount of time) to reverse for another party that might have been listening in them. The sender and receiver now use this common secret key to encrypt and decrypt their sent and received data.

Compared to traditional cryptosystems like RSA, ECC offers high security with smaller key sizes, which results in faster computation; lower power consumption, as well as memory and bandwidth savings. This is especially useful for mobile devices which are typically limited in terms of their CPU, power and network connectivity.A. Liu and P. Ning proposed "TinyECC: A configurable library for elliptic curve cryptography in wireless sensor networks [16], in this authors proposed Elliptic Curve Cryptography which has recently gained a lot of attention in industry. The principal attraction of ECC compared to RSA is that it offers equal security for a smaller bit size, thereby reducing processing overhead. ECC is ideal for constrained environment such as pager, PDAs, cellular phones and smart cards. For the implementation of elliptic curve cryptography (ECC) the plaintext encoding should be done before encryption and decoding should be done after decryption. ECC Encryption and Decryption methods can only encrypt and decrypt a point on the curve and not messages. The Encoding (converting message to a point) and Decoding (converting a point to a message) are important functions in Encryption and Decryption in ECC. It gives the details about Koblitz's method [14] to represent a message to a point and a point to a message. It provides mathematical formulas for encryption and decryption of messages.ECC algorithm [10] Compared to other public key cryptography counterparts like Diffie-Hellman (DH) and Rivest Shamir Adleman (RSA), Elliptic Curve Cryptography (ECC) is known to provide equivalent level of security with lower number of bits used. Reduced bit usage implies less power and logic area are required to implement this cryptographic scheme. This is particularly important in wireless networks, where a high level of security is required, but with low power consumption. This paper presents the implementation of Elliptic Curve Diffie-Hellman (ECDH) key exchange protocol over GF (2163). The Elliptic curve cryptography an emerging favorite because it requires less computational power, communication bandwidth, and memory when compared to other cryptosystems.ECC is a lightweight public key cryptographic (PKC) solution which is denoted with standard curve parameters and suitable for securing constrained. We use ECC-based implicit certificatesand Elliptic Curve Diffie-Helmann (ECDH) algorithm for the secure key establishment in unicast communication in WSNs. An influenced variant of Elliptic Curve Integrated Encryption Scheme (ECIES). ECIES is a hybrid encryption scheme that uses the functions such as key agreement, key derivation, encryption, message authentication, and hash value computation. ECC is a lightweight public key cryptographic (PKC) solution which is defined with standard curve parameters and suitable for securing constrained devices [10]. In fact the protocol 1 is an ECC variant of reference [11] with improvements (e.g., ensure the integrity and the authenticity of data, and remove the MITM attacks). Protocol 2 is a further optimized variant of the solution in [2], [11], and [12], and an influenced variant of Elliptic Curve Integrated Encryption Scheme (ECIES). ECIES is a hybrid encryption scheme that uses the functions such as key agreement, key derivation, encryption, message authentication, and hash value computation. Protocol 2 exploits the simplified functionalities in ECIES.

3. Multicast Routing Protocol

Use of multicast is of great interest, it is used to send the same report to several sinks. Multicasting is introduced to reduce bandwidth consumption in the network for various applications which include data replication, assignment of tasks and sending of commands to a specific group of sensors, queries to multiple sensors etc. Fire monitoring network is an example of multicast routing as in this network

sensors are deployed in a building to detect the probability of fire. If a building catches fire at some point then the sensors will sense the smoke or abrupt rise in temperature at that location. Further the sensed information is sent to a number of nearby sensors at other parts of the building to adjust their sampling rate and information the of fire responders such as fire brigade office, ambulance service, hospitals etc. Hence multicasting is done to allow the fire rescue team to start their operations in time with more efficiency. Earlier, the unicast routing protocols were there which were effective to provide unicast routing in resource-constrained scenarios, adapt very fast to challenging network conditions, overhead in a network should be low due to limited battery, storage capacity, bandwidth and processing power of sensor nodes, so there was a need to have such effective routing to alleviate the overall consumption of resources in the network as here in multicast routing the few copies are sent to the all destinations as possible of each datagram. The use of minimal amount of control information is there.

3.1 Approach for Multicast Routing

There are different configuration techniques proposed to support multicast routing but the four approaches for multicast routing are discussed. The proposed multicast routing protocols are based on one of these approaches and inherit their features. In the following section, an insight is provided to these techniques prior to proceed for discussion on Multicast routing protocols.

1.Tree Based Approach. This approach provides shortest and loop free paths and it is easy to leave or join a multicast group. Multicast tree is constructed on the basis of different parameters such as hop count and link quality indicator like delay, bandwidth or aggregated weight of the parameters. One of the drawbacks of this approach is that if any link failure occurs then this may cause the isolation of complete branch from the tree which may further contain multiple nodes.

2.Mesh Based Approach. Here all the group members form mesh connectivity in order to achieve a connection of every member with other members. Here route discovery and mesh construction is accomplished through broadcasting central points. This is more reliable and robust approach especially when the nodes mobility increases; moreover it estimates the traffic problems. Here if there is any link failure then the overall communication is not affected.

3.Geo-casting Based Approach. Geo-cast communication is limited to the destination nodes as the data packets are delivered to a set of nodes lying within a specific geographical area. The geo-cast group management is defined with the help of its geographic location. In heterogeneous networks this approach works efficiently but still there are some scalability concerns which are not suitable for large networks.

4.Rendezvous Based Approach. Here a subset of a node or a single node acts as rendezvous point (RP) in the network. The RP's are there to collect the sensed data from different sensor nodes and further transfer them to the sink nodes. A disadvantage of this approach is that it is a time consuming process and a big damage to the network occurs if RP failed.

Wireless applications, like emergency searches, rescues, and military battlefields where sharing of information is mandatory, require rapid deployable and quick reconfigurable routing protocols, because of these reasons there are need for multicast routing protocols. There are many characteristics and challenges that should be taking into consideration when developing a multicast routing protocols, like: the dynamic of the network topology, the constraints energy, limitation of network scalability, and the different characteristics between wireless links and wired links such as limited bandwidth and poor security. Generally there are two types of multicast routing protocols in wireless networks. Tree-based multicast routing protocol. In the tree-based multicasting, structure can be highly unstable in multicast ad-hoc routing protocols, as it needs frequent re-configuration in dynamic networks, an example for these type is Multicast extension for Ad-Hoc On-Demand Distance Vector (MAODV) [5] and Adaptive Demand- Driven Multicast Routing protocol (ADMR). The second type is mesh-based multicast protocol. Mesh-based multicast routing protocols are more than one path may exist between a source receiver pair, Core-Assisted Mesh Protocol (CAMP) and On-Demand Multicast Routing Protocol (ODMRP) are an example for these type of classification.

3.2 Multicast routing categories

Multicasting is a technique used to reduce the energy consumption in the network with the property of sending few copies as possible of each datagram to reach all destinations. This section of the paper focuses on three multicast routing protocols. Categories as illustrated below:

1. Tree Based Multicast Protocols: These protocols deliver multicast packet which relying on forwarding states that need to be maintained at nodes within a path. The drawbacks are control information flooding and storage for providing table establishment and maintenance which results in overhead in WSN.

2. Location Based Multicast Protocols: The multicast packets carry the location information of the destination nodes. It is beneficial in reducing the computation at every forwarding node in a path while searching for next forwarding node which results in excessive processing of CPU and energy consumption.

3. Source Based Protocols: These protocols make a path tree at a source and a multicast packet is encoded with the path tree, information is propagated which requires no states in WSN nodes. There are many source based, tree based and location based algorithms for routing with some advantages and disadvantages.

3.3 Challenges

As in WSN energy, memory and CPU power is limited; similarly in wired networks routers are responsible for handling packet replication and forwarding. The management for multiple groups and multicast trees requires memory and processing power, so for WSN it is not feasible to have overlay connection establishment all the time which results in higher energy consumption and hence network lifetime is reduced.

4. Protocol 1

The message flow of multicast key establishment of protocol 1 is shown in Figure below. Although the initiator injects the broadcast messages to start the key establishment, only the legitimate members of them unicast group are eligible to continue the rest of the process of key derivation.

Step 1: Initiator I determines the set of sensor nodes by their identity that should be included in the particular multicast group, and starts the communication. Accordingly, first the size of the multicast network (n), and the list of members in the multicast group U = {U1;U2; …. ;U(n-1)} are defined by the initiator. Then a random number ri εZp*is generated for the particular multicast session in order to obtain the freshness of each session and Ri= riGis computed. The broadcasting message is created using I's public key Qi = diG, Ri, and U. Later, the message {Qi; ri;U} is broadcast to the entire network along with the digital signature of the message, in order to announce the initiation of the multicast communication. Digital signature is computed as stated. Parameter Ri protocol 1 is reused for the parameter R in the signature scheme, whereas parameter Y in the signature scheme should be freshly obtained

Step 2: When the initial message is received by the sensor nodes in the network, first the list U is checked by each node to verify whether the particular node is included in the multicast group. If the node identity Uj, for j = 1; 2 ; … ; n - 1, is included in the list, the message is further processed, else it is discarded. The integrity of the received message is verified from the digital signature value. A freshly generated random number rjε Zp*and Rivalues are used to compute RijEC point, Rij= rjRi. Rj= rjGis also calculated for using shortly. Rijvalue, Uj's private key dj, and initiator's public key Qi are used to compute the secret EC point Sj: Sj=djQi+Rij. Afterwards, Ujcomputes Auth j= h(Sj‖Rij‖Uj), and sends{Rj;Qj; Authj;Uj} to the initiator as a response.

Step 3: Initiator I collects the responses received from all the responder sj= 1 to (n-1). If there is a loss of responses from the listed nodes in the multicast group, the initiator re-sends the same message after a retransmission time-out. For the retransmission it can use the same sequence number with a different epoch according to the DTLS handshaking mechanism [9]. However, further information about the retransmission is not provided, since it is out of scope of the main goal of the protocol design. After receiving the message from responder Uj, EC point Sj* is computed by the initiator. The rjand Qjvalues are used from the received message.Rij* = ri.rj mod p; Rij* = rij*G; Sj*= diQj+Rij*. Then the initiator checks Auth j=h(Sj*‖Rij*‖Uj). If the verification is successful, the intiator can proceed to the next step. Otherwise, it discards the message and re-sends the same multicast initiation request to those particular sensor nodes. If the verification result is still not successful for there transmissions of a certain node, then the initiator discards that node from the multicast group.

*Step 4:*As afore mentioned in step 3, the initiator I computes the respective SjEC points (i.e., shared secrets) for all the nodes of the multicast group. EC point Sj= (xj,yj) is encoded into the point (uj; vj) as follows: uj= h(xj);vj=h(yj). Next, for j ε {1; : : : ; n – 1}, the value uj={i=j ui}vjare computed. The set P = (u1‖ … ‖un-1)is determined and the multicast group key is then defined a sk=h(iui).

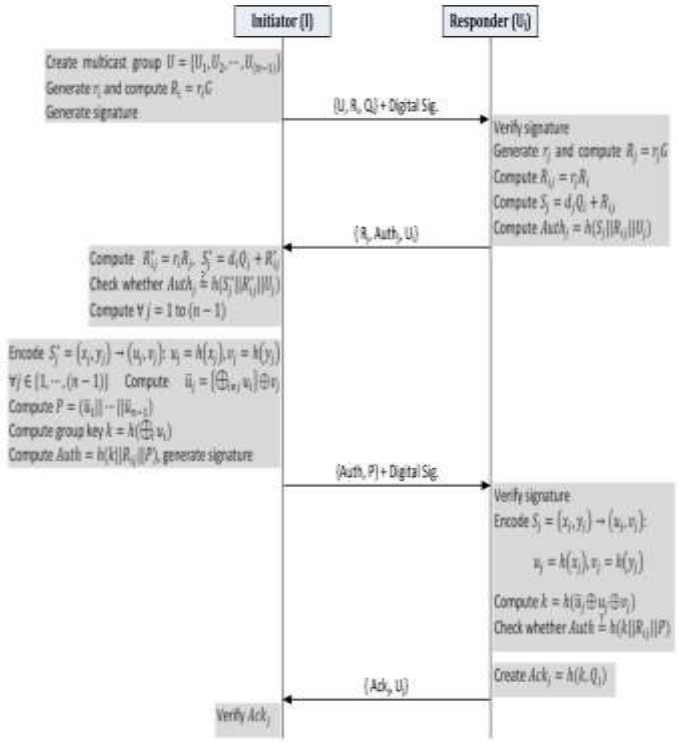

Fig 4.1 Message flow in protocol 1.

The new Authcode is now calculated as follows :Auth= h(k‖Rij‖P). Afterwards, the initiator broadcasts the message Auth; P along with the digital signature, which is computed. The random value Riis reused as parameter R in the signature scheme.

*Step 5:*When a responder node Ujreceives the second broadcast message, it first verifies the digital signature. The responder Ujuses Sjto compute (uj, vj) point. Next, the key k can be derived by k = h(uj, uj, vj). Then Ujverifies whether Auth= h(k‖Rij‖P). If this is correctly verified, then the group key k is authenticated.

*Step 6:*Each sensor node should send an acknowledgement message h(k,Qj) to finish the handshake. This ensures that every group member has correctly derived the group key k. After six steps, the initiator I and the other members of the multicast group U are having a common secret key k that can be used for multicast communication among the group.

5. ECIES Protocol

Protocol 2 exploits the concepts of ECIES to establish a shared secret key among the multicast group.

*Step 1:*First, the size (n) and the composition of the multicast group U = {U1;U2; …..;U(n-1)} are determined by the initiator as done in step 1 in protocol 1. Then a random value r is generated, where R = rG. EC points Sj are computed using r and the public keys Qjof the group members: Sj= diQj+R, where j = 1 to n - 1. Similar to protocol 1, EC point Sj= (xj,yj) is encoded into the point (uj; vj) as follows: uj= h(xj); vj=h(yj). Similarly, for j E {1; …. ;n-1},the values uj= {i!=j ui} vjare computed and denoted in the set P = (u1‖ ….. ‖un-1). The secret key is then defined as k = h(iui). The Authcode is calculated as follows: Auth= h(k‖R‖P).The new multicast message for group U is generated and transmitted by the initiator with the calculated values and the counter value C as follows: (Auth;C; R;U; P). Additionally, the digital signature is

appended to preserve message authentication and integrity. The same R value can be reused as the parameter R in the signature scheme.

*Step 2:*When the sensor node Ujreceives the broadcast message, initially, it checks whether it is included in the multicast group U. Then the digital signature and the counter Care checked. If both are correctly verified, Sjis computed using the received random value R and node's private key dj:Sj= djQi+R. The EC point Sjis converted to the point (uj,vj) using the same encoding as in step 1. Next, the key k is derived by k =h(uj,uj,vj). Similarly, all the nodes in the group have to proceed the same computations to derive the group key. Then Ujverifies whether Auth=h(k||R||P). If this is correctly verified, then the group key k is authenticated.

Step 3: Each sensor node should send an acknowledgement message h(k,Qj) to finish the handshake. Later, by verifying the acknowledgement message, the initiator can ensure the authenticity of the particular group member and the accurate derivation of group key k. After three steps the shared secret key is known by the initiator and the other members in the multicast group. Compared to protocol 1, this protocol 2 is more efficient and creates lower overhead on the sensor nodes due to less message transactions and reduced number of operations at the responder ends.

Fig 4.2 Message flow of protocol 2.

For the key establishment, the number of message transactions between the initiator and a responder group member is four for protocol 1 and two for protocol 2. Additionally, the number of operations performed at each end, the number of message transactions, and the overhead are also less in protocol 2 than that of protocol 1 as shown in Table 1.This increases the efficiency and performance of the second proposed protocol. However, in both protocols, the group key has to be re-established after the addition of a new node or the removal of an existing node. In both protocols, in order to provide group and initiator authentication, the group key is derived with the contribution of the multicast group members. This is an implicit assurance that all nodes contribute and authorize the final group key. However, in protocol 1 the group members provide greater contribute onto the key derivation with a higher degree of randomness, whereas in protocol 2 the initiator performs the majority of the operations. Protocol 2 is first taken into account for discussing the scalability features as it has less message transactions. The actions are described with respect to the key refreshing when a new member joins or an old member leaves the group. When a new member Uxjoins, the initiator node needs to compute Sx= diQx+R. Otherwise a unicast message needs to be sent to Ux. The corresponding EC point (ux, vx) is derived from Sx. Next a new randomKey k is derived. The rest of the protocol remains the same. The difference with key refreshing is that n - 1 less point multiplications need to be performed in order to derive the points associated to the group members since those points are pre-calculated. The message length on the other hand slightly increases with one extra value for uxand the length of the identity Ux. On the other hand when a member Uoleaves the group, the initiator node needs to determine a new group key k, using the n - 2 remaining values of ui. Now the transmission can be simplified, since only an updated version of C, the point R, the removed user Uo, together with an authentication tag, and a signature need to be sent. As a consequence, the message length reduces by (n-1) * 20+(n-2) *2 Byte. This is only valid, if the node stores the information of those points related to the users. Similar adaptations are performed in protocol 1at node addition and node removal. The significant difference in the node addition in protocol 1 is that message 1 and 2are unicast message exchanges between the initiator and new node Ux. The initiator computes only the new EC point Sxn and reuses the remainder of the pre-computed (n-1) points. When leaving a member in protocol 1, the initiator can reuse the pre-calculated (n - 2) points and determine a new group key k.

6. Results

The simulation output has been tested with NS2 simulator. The results are compared with Protocol 1 and ECIES. In order to evaluate Protocol 1, ECIES and ECIES Enhancement the network setup was executed with 3 multicast groups considering 10 nodes in each group with 3 source nodes. It has been found that ECIES outperforms then protocol 1, in all the comparison of parameters like overhead, cost and packet delivery ratio. ECISE gives best results than protocol 1 were in ECIES enhance a new sink node joins the group and it is observed that overhead is slightly increased in ECIES enhance compared to ECISE.

6.1 Parameters of Simulation

6.1.1 Packet delivery fraction: This is defined as the ratio of the number of packets received at the destination and the number of packets sent by the source.

6.1.2 Overhead: Overhead is the number of routing packets required for network communication.

6.1.3 Cost: This is defined as the lifetime per unit cost n as the network lifetime L divided by the number of deployed sensors N.

6.2 Data transmission process: Here we can see that after successful multicast registration completed then secure communication is started between source and sink nodes present in all the 3 groups. The communication between one group to other group can not be done as admin generates public and private keys to all the source nodes which is confidential.

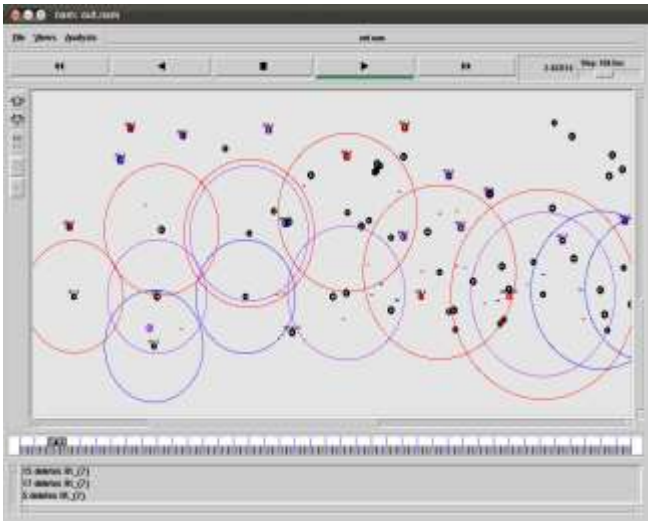

Fig 6.1.Communication between all the source nodes and sinks nodes present in the network.

6.3 Graphs

XGraphs are used for analyzing output.

Packet delivery fraction: From the Analysis we can see that in case of Protocol 1, the packet delivery is very low. But in case of ECIES, ECIES enhance the packet delivery ratio against different number of nodes is more when compared to Protocol 1 in our analysis.

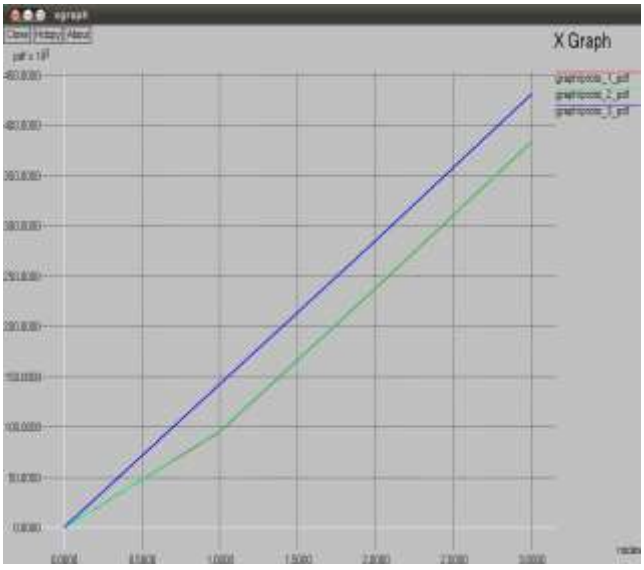

Fig 6.2 Analysis of protocol 1, ECIES and ECIES enhance in case of packet delivery ratio for 100 nodes.

Overhead: From the analysis we can see that in case of protocol 1, the overhead is high. But in case of ECIES the overhead is less when compared to protocol 1 in our analysis, were in ECIES enhancement overhead is slightly increased compared to ECIES because a new node joins the group.

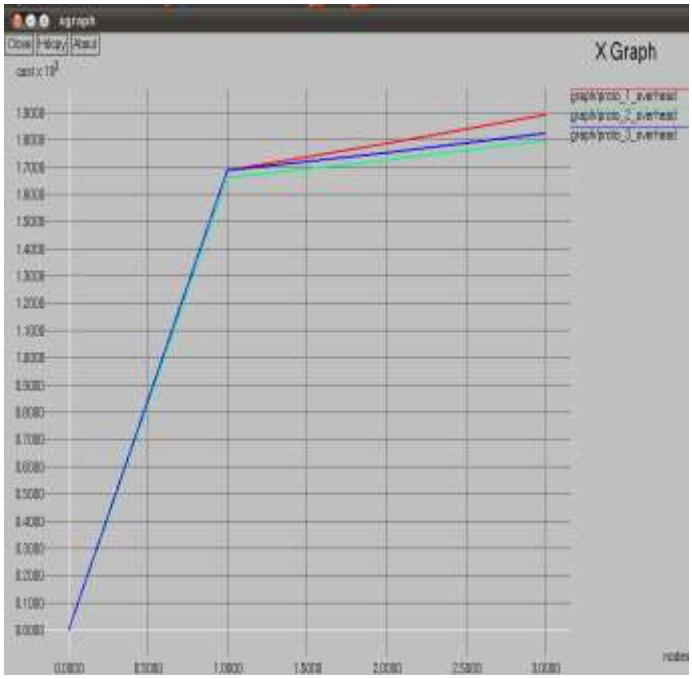

Fig 6.3 Analysis of protocol 1, ECIES and ECIES enhance in case of Overhead for 100 nodes.

Cost: From the Analysis we can see that in case of protocol 1, cost is very high. But in case of ECIES cost is less compared to protocol 1 in our analysis, were in ECIES enhancement cost is more compared to ECIES because a new node joins the group.

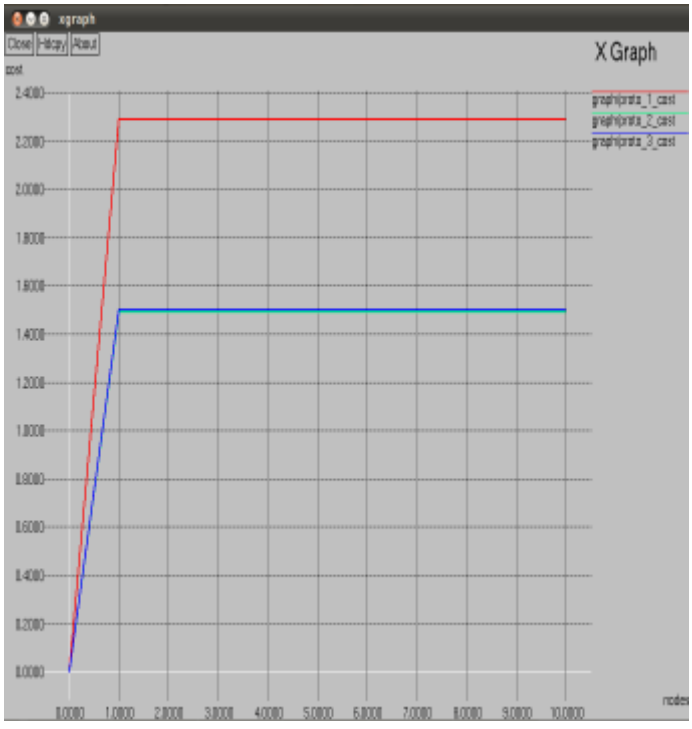

Fig 6.4 Analysis of protocol 1, ECIES and ECIES enhance in case of Cost for 100 nodes.

6.4 Table

Table shows the comparison values between 3 protocols in all the given parameters.

	Protocol 1	ECIES Protocol	ECIES enhance
Packet delivery fraction	569800	598775	627263
Overhead(bytes)	9863	9588	9740
Cost(sec)	2.29	1.49	1.5

7. Conclusion and Future Work

Two secure group key protocols are formed for multicast communication in WSNs. The key can be further used for securing multicast messages. ECIES Protocol always performs better than protocol 1, because in protocol 1 more cryptographic operations are performed for multicast communication when compared to ECIES protocol. When a new node wants to join the group, it is observed that overhead is slightly increased. Protocol 1 is more appropriate for distributed applications, which require group members to highly contribute to the key computation and need greater randomness. Since the energy cost at the responder side is very low, ECIES protocol is more suitable for centralized applications, where mostly cryptographic operations are performed by a central entity and edge nodes have very low energy profiles. The two protocols proposed are expected to be extended to many-to-many (m :n) communication scenarios obtaining comprehensive quantitative results for real-time test-beds.We have analyzed the performance of the both protocols under different network parameters like cost, overhead, and packet delivery fraction. ECIES Protocol always outperforms protocol 1.

References

[1] "Group Key Establishment For Enabling Secure Multicast Communication In Wireless Sensor Networks Deployed For Iot Applications" Pawani Porambage1, An Braeken2, Corinna Schmitt3, Andrei Gurtov4, (Senior Member, Ieee), Mika Ylianttila1, (Senior Member, Ieee), And Burkhard Stiller3

[2] L. Harn and C. Lin, ``Authenticated group key transfer protocol based on secret sharing," IEEE Trans. Comput., vol. 59, no. 6, pp. 842_846,Jun. 2010.

[3] J.-H. Son, J.-S.Lee, and S.-W. Seo, ``Topological key hierarchy for energy effcient group key management in wireless sensor networks," WirelessPers.Commun., vol. 52, no. 2, pp. 359_382, 2010.

[4] X. Cao, X. Zeng, W. Kou, and L. Hu, ``Identity-based anonymous remote authentication for value-added services in mobile networks," IEEE Trans.Veh. Technol., vol. 58, no. 7, pp. 3508_3517, Sep. 2009.

[5] "Multicast routing with AODV Routing protocol" Aki AnttilaCygate Networks Vattuniemenkatu 21, P.O.Box 187, 00201 Helsinki, Finland .

[6] S. Keoh, S. Kumar, O. Garcia-Morchon, E. Dijk, and A. Rahman. (Feb. 2014). "DTLS-Based Multicast Security for Low-Power and LossyNetworks (LLNs)".

[7] P. Porambage, C. Schmitt, P. Kumar, A. Gurtov, and M. Ylianttila, "Two-phase authentication protocol for wireless sensor networks in distributed IoT applications," in Proc. IEEE Wireless Commun. Netw.Conf. (WCNC), Apr. 2014, pp. 2728_2733.

[8] A. Perrig, D. Song, R. Canetti, J. D. Tygar, and B. Briscoe. (Jun. 2005). "Timed Efficient Stream Loss-Tolerant Authentication (TESLA)": Multi-cast Source Authentication Transform Introduction.

[9] T. Kothmayr, C. Schmitt, W. Hu, M. Brünig, and G. Carle, ``DTLS based security and two-way authentication for the Internet of Things," Ad HocNetw., vol. 11, no. 8, pp. 2710_2723, 2013.

[10] Elliptic Curve Diffie-Hellman Protocol Implementation Using Picoblaze: MakhamisaSenekane†, SehlabakaQhobosheane, and B.M. TaeleIJCSNS International Journal of Computer Science and Network Security, VOL.11 No.6, June 2011

[11] C.-Y. Lee, Z.-H.Wang, L. Harn, and C.-C. Chang, ``Secure key transfer protocol based on secret sharing for group communications," IEICE Trans.Inf. Syst., vol. 94, no. 11, pp. 2069_2076, 2011

[12] Efficient and Secure Source Authentication for Multicast: Adrian Perrigy_ Ran Canettiz Dawn Songy J. D. Tygary UC Berkeley, _Digital Fountain, zIBM T.J. Watson fperrig,dawnsong,tygar@cs.berkeley.edu, canetti@watson.ibm.comg

[13] Multicast Routing Protocols for Wireless Sensor Networks:A comparative studyKanchanVerma International Journal of Computer Science and Innovation Vol. 2015, no. 1, pp. 39-52ISSN: 2458-6528

[14] Padma, D.Chandravathi, P.PrapoornaRoja proposed "Encoding And Decoding of a Message in the Implementation of Elliptic Curve Cryptography using Koblitz's Method in 2012".

[15] A.Liu and P.Ning[13], proposed "Tiny ECC: A Configurable Library For Elliptic Curve Cryptography In Wireless Sensor Networks" , CSE dept, King Fahd University of Petroleum and Minerals in 2008.

[16] Ram RatanAhirwal, ManojAhke "Elliptic Curve Diffie-Hellman Key Exchange Algorithm for Securing Hypertext Information onWide Area Network" International Journal of Computer Science and Information Technologies, Vol. 4 (2) , 2013, 363 – 368.

DOI: 10.18535/ijecs/v6i4.10

Author Profile

MissP.Prasanna Laxmi isdoing M.Tech in Computer Science and Engineering at MVSR Engg College under Osmania University, Hyderabad and received B.Tech in Computer Science and Engineering from JNTUH in 2014

MrsM.Anupama is currently working as an Associate Professor at MVSR Engineering College, Hyderabad in the Department of Computer Science and Engineering. She has a teaching experience of over 23 years. She obtained her B.Tech from Nagarjuna University,Guntur andM.Tech from JNTUH. She is presently pursuing her Ph.D. from RayalaseemaUniversity, Kurnool in AdhocWireless Networks. Her areas of interest include Computer Networks ,Network Security, Mobile Computing and Image Processing.