International Journal of Advanced Science and Technology
Vol. 29, No. 12s, (2020), pp. 816-822

Energy Efficient Secure Multicast Group Communications For Iot Applications Using WSN

Kartheeban K[1], Vairachilai S[2], Shubhangi V Urkude[3]
[1,2]*Department of Computer Science and Engineering,*
[3]*Faculty of Science and Technology*
[1]*Kalasalingam Academy of Research and Education, Krishnankovil, Tamilnadu, India*
[2,3]*The ICFAI Foundation for Higher Education (IFHE), Hyderabad, Telangana, India*
Email: [1]k.kartheeban@klu.ac.in, [2]vairachilai@ifheindia.org, [3]ushubhu@ifheindia.org

Abstract

Internet of Things (IoT) is the latest industry buzzwords and it uses actuator networks (WSNs) as its backbone. Using node-to-node communication in the form of multicasting and broadcasting is needed in the energy-constrained nodes in IoT. To make secure group communication for the group of nodes we propose a less energy efficient protocol for making a secured multicast group communication using WSN. The applications of this protocol is examined and rationalized by a systematic analysis of the performance metrics based on three different parameters such as packet loss, overhead and cost using NS3 simulation based on different destination nodes.
Keywords: *Secure Group Communication, Internet Of Things, Wireless Sensor Networks.*

1. Introduction

Actuator networks are spatially distributed individual sensor to collect environmental factors and pass these data to the network in other locations. Establishment of group key in a secure manner is a major concern to provide confidentiality, authentication, and integrity for transmissions of message in these groups. Apart from controlling the sensor activity, the modern networks are also bi-directional. There are different applications of sensor networks such as battlefield surveillance, industrial process monitoring, and control, machine health monitoring etc. Routing protocols are used to transmit messages from sources to destination in wireless sensor network and it having three types such as unicast, broadcast and multicast. The unicast is used to send a message from one source to one destination (One-to-One). Similarly, the broadcast is used to send a message from one source to selected destinations (One-to-All). Finally, the multicast is used to send a message from a source to multiple destinations (One-to-Many). The prime objective of multicast is, similar message will be sent to all links. The use of multicasting is minimization of bandwidth in the network for many applications that comprises redundant of data, allocation of work.

In a sensor network, there are several sensor nodes are used to gather the data and the collected information will be transmitted to the base station. There are two types of sensor networks such as distributed and hierarchical. Grouping of pair keys is a major constrain in hierarchical wireless sensor network (HWSN) among the nodes using the factors such as cluster heads, sensor nodes and base stations. Each sensor has less memory size, limited batter power, data processing capability, and short radio transmission range. Sensor nodes in a cluster (also called a group), communicate each other in that clusters and finally responds to the commands from the cluster head (CH). Usually, Cluster heads are equipped with more resources such as compared with sensors, which are equipped with dominant antenna, huge batteries power, and memory. It is very much significant to encrypt all messages before transform among sensor nodes in wireless sensor networks to achieve security and the encryption keys would be concurring depend upon the communicating nodes. Achieving key agreements among communicating nodes in wireless sensor networks is nontrivial due to constraints of resource. Diffie-Hellman and public-key based schemes are some of the key agreement schemes available for general

networks and these schemes are not suitable for resource constraint wireless sensor networks. Due to the huge consumption of memory and the size of network, the pre-distribution of secret keys to all the nodes is not suitable method. In the recent research a pre-distribution schemes based on improved random key have been proposed and it does not require any deployment knowledge.

Key establishment, distribution, and management are main important functions of security protocols in wireless sensor networks. The traditional asymmetric key cryptosystems are not feasible in wireless sensor networks, due to strict constraints on the recourses. Many researchers show that pre-distributing pair-wise key into the sensor networks before deployment is always best mechanism to solve key establishment issues. This particular work focus on prior distribution of pair wise keys in wireless sensor nodes and to deals with the key establishment problem. Pre-distribution keys based on the random method provide based on the probabilistic approach and the resilience of network. To provide low communication and computational overhead, an efficient pair wise management scheme and key establishment to be used to attain both resilience and connectivity of network in static networks. Since the wireless sensor networks (WSN) are implemented in an unstable environment, the legitimate users can access data after login and when needed. In general, the wireless sensor network consists of one base station and thousands of sensor nodes connected with the base station and these sensors are used in the network to monitor targeted area and sense information from that area according to the applied application and transform this data to the base station. Sometimes the intruder can insert false information in the network or steal the routing information between nodes and base station or between nodes. This implies that security is an important constrain in the sensor networks. Therefore, user authentication is one such important issue before the data is accessing from the sensor nodes in the wireless sensor network.

2. Problem Definition

Sensor nodes act as IOT devices in Wireless sensor networks, which involved in reducing the energy requirement and processing complexity in the network. In WSN, sensor nodes are formed together to create sensor node groups. The main goal of group formation is to achieve efficient data sharing between the group member nodes. In previous work, there is more packet overheads occurs during the time of the secret key sharing which leads to higher amount of packet loss. To solve this problem, a new solution is prepared to improve the data sharing between the group members by efficient group formation. Our proposed system establishes a secure secret key and that will be shared among the group by generating authentication code which is based on the addition of the list, random number and secret key point.

3. Proposed System

The proposed system deliberates on establishing a connection in multicast group by communicating the shared secret key. Here we introduce the protocol, Integrated Encryption Scheme based on Elliptic Curve (ECIES) that allows exchange of key, encryption, and authentication of message and Computation of hash value. Primarily, the starter measures the number of nodes in the IoT group by using its ID and then the communication starts between the nodes in the group. The initiator public key is used for broadcasting the messages. The message is broadcast to the whole network along with the authentication code and the digital signature that is incorporated to protect message authentication and security. Initially, when the sensor node receives the message first it verifies that this node is a part of the group. Secondly, it checks the authentication code and digital signature. The authentication code is generated by adding the list U, random number R and the secret key point S that reduces the overhead of the packets during the key sharing. The adding process of these three entities reduces the packet loss. Group key is authenticated, if all the nodes in the networks are verified correctly. If all the nodes completed the handshake, then the acknowledgement should be sent. The initiator ensures the authentication of group key is shared among the group members after verifying acknowledgement message.

4. Methodologies

4.1 Authentication

In our paper, elliptic curve points are generated by using random value and public key value. Then the elliptic curve points are encoded for security concern. Then the authentication code is calculated. Finally, authentication code and digital signature is encrypted by ECIES.

4.2 Key Generation

Secret key is generated by a common host and it is distributed among the group members. To avoid the authentication of message and integrity the digital signature mechanisms were used. The same values can be salvaged as parameter (R) for the signature scheme.

4.3 Key Distribution

The secret key is distributed among the special multicast group and the verification process among the multicast group members are processed.

4.4 Verification

Each sensor node receives the message with authentication code and digital signature. Initially, each sensor nodes checks, if it is a member of a group and then it verifies the authentication code and the digital signature. If all the nodes completed the handshake, then the acknowledgement should be send. The initiator ensures the authentication of group key is shared among the group members after verifying acknowledgement message.

4.5 Performance Evaluation

The performance of key establishment for multicast group communication is evaluated by following parameters.

- Packet delivery ratio
- Overhead
- Cost

5. Architecture

The System Architecture is shown in Figure 1.

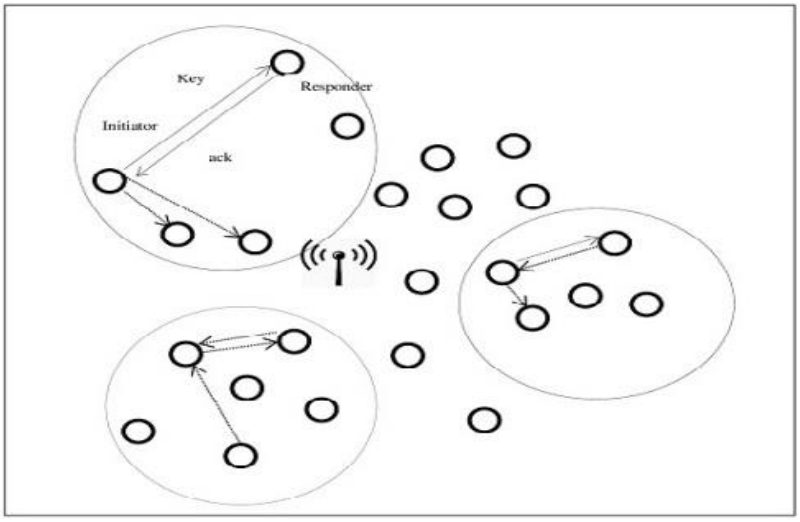

Figure 1. System Architecture

6. Results

The simulation output tested with NS3 simulator. The results are compared with both the algorithms. In this project, we used 50 sensor nodes to setup sensor network. After construct the sensor networks, we focuses to enlarge the lifetime of the created networks used in wireless. The dynamically moving sensor nodes are grouped to form a multi-cast group and perform multi-cast communication. It has been compared with Packet Delivery Ratio Vs Nodes, Cost Vs Nodes, and Overhead Vs Nodes.

6.1 Parameters of Simulation

6.1.1 Packet delivery ratio The calculation of this parameter is based on. The count of packets delivered by the source and count of packets delivered by the destination is used to calculate packet delivery ratio.

6.1.2 Overhead It is calculated based on sum of packets implicated in the multicast group communication for each separate group.

6.1.3 Cost This is the lifetime for each routing packets in the network communication.

6.2 Simulation Process

In this group of nodes are created and they are involved in the communication between these nodes. Among them, one of the nodes creates the public key and distributes. Each member will assume a random number and then distributes to them. The creation of nodes shown in Figure 2 and the Communication of group of nodes shown in Figure 2.

6.3 Graphs

Packet Delivery Ratio (PDR): From the graphs obtained, we analyse that the packet delivery ratio in both the algorithms are equal. Hence, same number of packets is compared in the two algorithms. The result is shown in Figure 4.

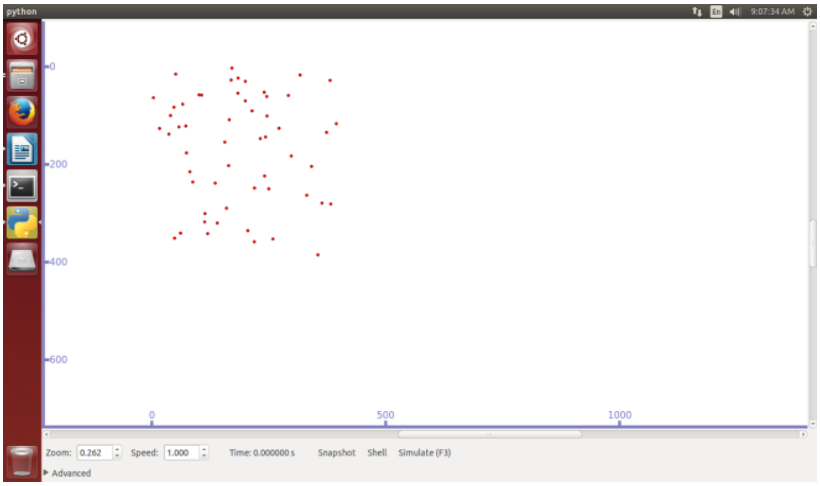

Figure 2. Creation of Nodes

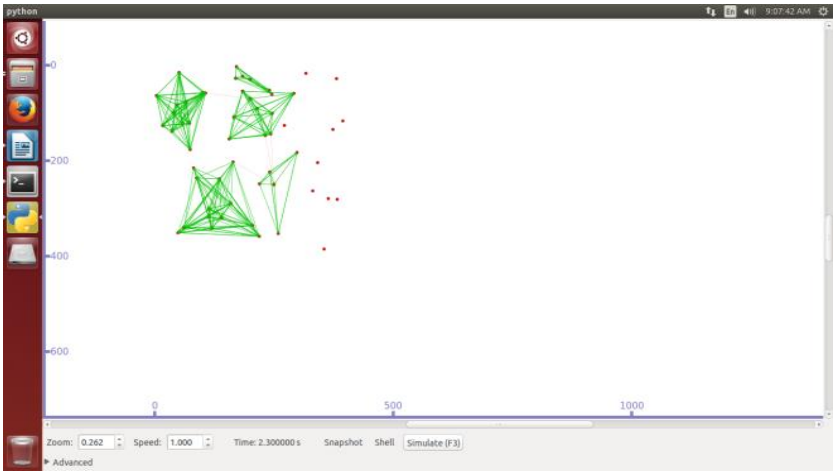

Figure 3. Communication of Group of Nodes

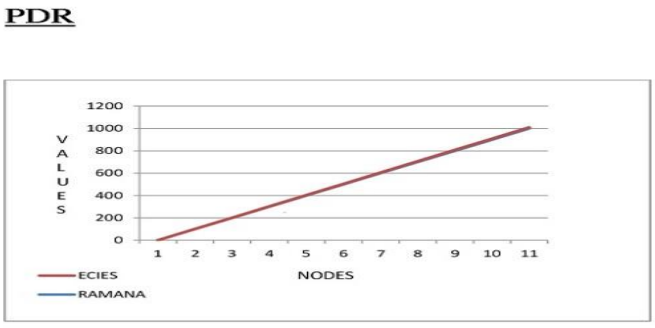

Figure 4. PDR graph

Overhead: From the graphs obtained, we analyse that the overhead ratio for both the algorithms are obtained. Here the units for the graphs are measured in bytes. The algorithm performance is higher than

the ECIES algorithm performance. Hence, the values are represented in the form of a table. The result is shown in Figure 5.

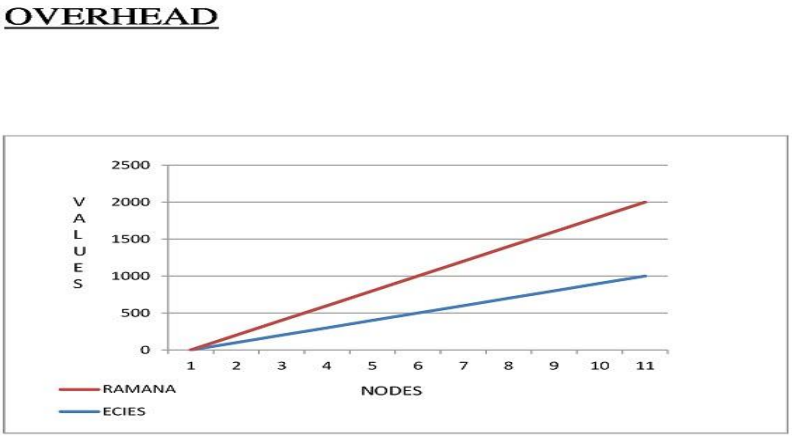

Figure 5. Overhead Graph

COST: From the graphs obtained, we analyse that the cost ratio for both the algorithms are obtained. Here the units for the graphs are measured in seconds. The algorithm performance is lower than the ECIES algorithm performance. Hence, the results are shown in the Table 1. The cost graph is shown in Figure 6.

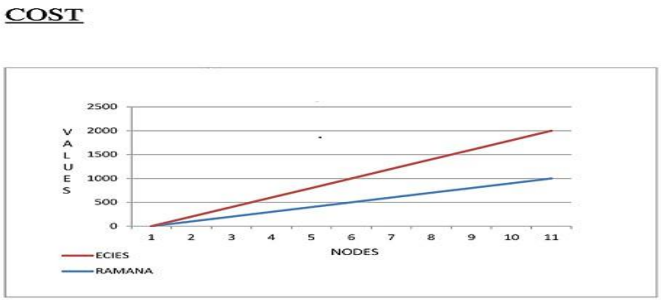

Figure 6. Cost graph

Table 1. Comparison of Two Algorithms

	COST (SECONDS)	OVERHEAD (BYTES)	PDR
ALGORITHM	1000	1600	4e+09
ECIES	1250	850	4e+09

7. Conclusion

This system establishes the group key for multicast network by using algorithm. A group key is generated for the multicast group members and distributed among them. The result shows that our algorithm performs more effective than the ECIES algorithm. The packet overhead and packet loss is reduced in the proposed system. The performance metrics shows that our proposed work produces better results than previous work. This is appropriate for more distributed applications in IOT. Hence, we analyse that our algorithm always gives better performance results compared with ECIES algorithm under different network parameters like packet delivery ratio, overhead and cost.

8. Future Work

We have planned to improve our project by following areas,

- Security can be further enhanced by using hybrid cryptography
- Minimization of energy consumption

References

[1]. Pawani Porambage, An Braeken, Corinna Schmitt, Andrei Gurtov, , Mika Ylianttila1, & Burkhard Stiller, "Group Key Establishment For Enabling Secure Multicast Communication In Wireless Sensor Networks Deployed For IoT Applications", IEEE Access, Vol.3, no.7, (2015), pp.1503-1511.
[2]. L. Harn and C. Lin, "Authenticated Group Key Transfer Protocol Based On Secret Sharin," IEEE Transactions On Computers, Vol.59, no.6, (2010), pp.842-846.
[3]. J.-H. Son, J.-S.Lee, and S.-W.Seo, "Topological key hierarchy for energy effcient group key management in wireless sensor networks," Wireless Personal Communications, Vol. 52, no. 2, (2010), pp. 359-382.
[4]. X. Cao, X. Zeng, W. Kou, & L. Hu, "Identity-based anonymous remote authentication for value-added services in mobile networks," EEE Transactions on Vehicular Technology, Vol. 58, no. 7, (2009), pp. 3508-3517.
[5]. Adrian Perrig, Ran Canetti, Dawn Song, & J. D. Tygar "Efficient and Secure Source Authentication for Multicast," proceedings of the Network and Distributed System Security Symposium NDSS 2001, San Diego, CaliforniamUSA, (2001) January 321-332 .
[6]. A.Liu & P.Ning, "Tiny ECC: A Configurable Library For Elliptic Curve Cryptography in Wireless Sensor Networks," proceedings of the international Conference on Information Processing in Sensor Networks,St.Louis,Missouri,USA(2008), April 245-256.
[7]. P. Porambage, C. Schmitt, P. Kumar, A. Gurtov, & M. Ylianttila, "Two-phase authentication protocol for wireless sensor networks in distributed IoT applications," Proceedings of the IEEE Wireless Communications and Networking Conference, (2014) pp. 2728-2733.
[8]. Perrig, D. Song, R. Canetti, J. D. Tygar, & B. Briscoe. "Timed Efficient Stream Loss-Tolerant Authentication (TESLA)":Multi-cast Source Authentication Transform Introduction," 2005.
[9]. T. Kothmayr, C. Schmitt, W. Hu, M. Brünig, & G. Carle, "DTLS based security and two-way authentication for the Internet of Things," Ad Hoc Networks, Vol.11, no.8, (2013), pp. 2710-2723.
[10]. Senekane, Makhamisa Qhobosheane, Sehlabaka & Taele, Benedict " Elliptic Curve Diffie-Hellman Protocol Implementation Using Picoblaze," International Journal of Computer Science and Network Security, Vol. 11, no.6, (2011),pp. 257-268.