Enhancing Security of Wireless Sensor Network in Group Communication by Secure and Effective Key Management System

Lavanya.S[1], Nithya.S[2], Pon Rajasree. P[3], Preethi. J[4], V.S.Kamalakkannan[5]
[1, 2, 3, 4, 5] Department of Electronics & Communication Engineering
[1, 2, 3, 4, 5]SNS College of Engineering, Coimbatore, India

Abstract-*Tracking a region is critical in actual international. For that, sensor used as community. a unicast communication is a direct one to one communication in which messages are dispatched to a single network .so ,we go for multicast conversation where facts is addressed to a collection of vacation spot concurrently and efficiently to a set in single transmission . In any community secure key control is used for its versatility(authenticity, integrity , and confidentiality) of the data Normally cryptography strategies are used for securing messages in stressed out and networks .On this paper we use ECC(elliptical curve cryptography)for at relieve multicast communication amongst many methods in ECC we use Elliptic Curve Implemented Encryption System(ECIES) that is a encryption scheme that uses the functions which include key agreement, key derivation, encryption, message authentication, and hash fee computation. Ns2 is used as a tool for simulation.*

I. INTRODUCTION

Networks of wireless sensors decide a key constructing block for tracking any network. Furthermore, sensors are devices that has restrained processing , and that frequently runs on batteries(e.g., low CPU clock and recollection track). Unicast messages to a single network in many copies consume more power. So it's far higher to send multicast messages to a collection of gadgets in a single replica that's more efficient and effective.The function of securing institution key status is to shape the key capability to offer integrity, authentication, and confidentiality for message transmissions in those multicast corporations. Multicast schemes may be carried out in lots of sensor networks together with clever homes, clever cities, environmental monitoring, and healthcare.

For a better understanding of primary necessities for a multicast aid the following use cases are decided. The first use case is designed for the control of mild bulbs in a clever constructing. The environmental monitoring community collects records about light intensity, temperature, and population of all rooms in the constructing and delivers aggregated records to a major entity. Primarily based on statistics obtained, the major entity can permit synchronous operations (e.g., giving instructions for on, off, or dim-stage) amongst a group of light bulbs in a ground or room to reach a visual synchronicity of light effects on the consumer. the second one use case is about the gathering and aggregation of patient information and sending out the facts required to relevant contacts (e.g., medical doctors or nurses). The aggregating unit collects statistics about the patient's ECG readings and blood strain. In flip, the processing unit determines the exact set of individuals, who ought to react in line with the statistics received, and defines them as a completely unique multicast institution. In these use instances, multicast businesses ought to be securely formed and respective secret keys have to be shared among all multicast group individuals to ensure secure communications.

II. SYSTEM VERSION

The time period multicast group stands for a selected institution of nodes, which might be interested in or allowed to receiving the common set of statistics or instructions. The entire range of nodes taken into consideration within the multicast network is n, which includes the initiator node and (n − 1) multicast group participants. In the following multicast group participants, additionally called the responder nodes.

A common secret key, which is known by the initiator and the responders, is used for comfortable communication within the multicast institution.

The important thing derivation is originated via the initiator and computed according to the inputs given through the responders. For this sort of situation, the size of the multicast community needs to be identical or greater than 4: n ≥ four. otherwise, It'd be greater while the initiator node derives the organization key and provides the key as unicast messages to each nodes.

A. Adversary version

For the sake of clarity, the conduct of the adversary version is described correlating to the use case of

controlling the lights manipulate state of affairs. In line with this case, an adversary can drop the controlling messages exchanged between the essential entity and the mild bulbs. It could fraudulently act as a valid intermediate tool in the course of the important thing establishment between the crucial entity and the mild bulbs, and launch MITM attacks. As a substitute, an adversary who is external or internal to the network may also retransmit the preceding key status messages to generate replay attacks and interrupt the regular operations of the light bulbs. If the adversary captures a light bulb, he may also discover the name of the game institution keys saved in the bulb.

B. Assumptions

Ordinarily, it is assumed that the underlying communication epoch and sensor nodes guide multicast organization formation and message transactions. Secondly, it is considered that all network entities own common place protection associations (i.e., cipher suites) and perform identical cryptographic operations (e.g., hashing (h()), encoding, deciphering). Common Elliptic Curve (EC) parameters are embedded in all of the network entities that take part inside the communication state of affairs. EC parameters are denoted through q, a, b, G, and p. The parameter q is a high, which shows the finite subject Fq. The variables a and b are coefficients of EC y2 = x3 + ax + b, wherein 4a3 + 27b2 6= 0. G is the bottom point generator with order of p, which is also a high . The initiator (I) is considered a prime powered resource rich entity (e.g., gateway node) and has higher processing strength and recollection ability than the rest of the nodes in the multicast organization. The initiator is likewise aware of the agreement of the institution (i.e., knowing the identities of the valid nodes). In each protocols, the initiator is supposed to recognise the public keys of all the nodes and vice versa. The snoozing patterns of the nodes and route losses inside the verbal exchange hyperlinks aren't being taken into consideration due to the fact that they're out of the scope of the key objective of this paper. Therefore, it is assumed that the participants of the multicast group will more rapidly or later obtain the initiator requests and the rest of the messages without screw ups.

C. Signature scheme

By incorporating signatures with the transmitting messages, they could make certain the houses consisting of integrity, authentication, and non-repudiation. Because the generic accessibility of IoT networks are acquired by means of IPv6 addresses, It'd be an brought benefit to make the most the device identities with the signature scheme. But, the standard Elliptic Curve digital Signature algorithm (ECDSA) does now not produce signatures with the node identities. The ECDSA scheme utilizes most effective the personal and public keys of the signee to experienced and verify the signature. Consequently, with a view to make the most device identities, the following green signature scheme is used.

D. Protocol analysis

The performance analysis is based at the estimated power intake of the computation and conversation strength cost of the protocols. The scalability analysis illustrates the protocol behaviors at node additions and removals. Protection evaluation explains how properly the proposed protocols can mitigate the maximum not unusual security threats and vulnerabilities. We also display a brand new MITM attack.

III. PERFORMANCE EVALUATION

For the key establishment, the number of message transactions among the initiator and a responder organization member is 4 for protocol 1 and for protocol 2. Additionally, the wide variety of operations done at every stop, the number of message transactions, and the overhead are also much less in protocol 2 than that of protocol 1 as proven. This will increase the efficiency and overall performance of the second proposed protocol. However, in each protocols, the organization key has to be re-mounted after the addition of a brand new node or the removal of an present node. In both protocols, to be able to provide group and initiator authentication, the organization key's derived with the contribution of the multicast group individuals (i.e., the group key is derived through the important thing components of each member). That is an implicit guarantee that every one nodes contribute and authorize the final group key. But, in protocol 1 the organization individuals offer greater contribution to the key derivation with a better diploma of randomness, while in protocol 2 the initiator plays most people of the operations.

Comparing to hashing and operations, EC factor operations (i.e., point addition and multiplication) are taken into consideration the most high priced calculations. Therefore, to be able to estimate the approximate energy consumptions for computation, message transmission, and message reception,We forget the ones operations that result in smaller impact on the entire electricity, and recall handiest the EC point multiplications (PM) and point additions (PA) in each step.

Hence, the computational overhead and the length of transmission and reception messages, at the same time as the multicast network size is n. Calculations are done for the

SECP160R1 curve ECC operations with the estimations together with EC point is 20 Byte, h() output is 16 Byte, node identification and counter C are 2 Byte, and fee P is sixteen Byte. The very last values additionally consist of the contribution of the virtual signature scheme as explained in Sections III-D and IV. Furthermore, inside the real implementation it is vital to perform the fragmentation of the huge messages, which exceed the maximum transfer unit size of the network (e.g., in IEEE 802.15.4 networks this would be 128 Byte).

Electricity charges are computed with respect to conventional Crossbow sensor nodes, which insert 4 MHz MSP430 microcontroller and follow the IEEE 802.15.4 requirements with a records fee of 250 kbps. Strength values are approximated contemplating that EC factor multiplication consumes 17 mJ and the point addition also has an upper sure of the equal fee. From the traits of the CC2420 transceiver used in Telos B sensors, the unit transmission and reception strength costs are respectively taken as zero.209 µJ and zero.226 µJ. For that reason the computation, transmission, and reception electricity consumptions are calculated for each protocols 1 and a pair of at the responder aspects through various the scale of the network n along with the TKH scheme . As depicted in the distinguish, the electricity costs of the key status at end nodes in our protocols are fairly decrease than the tree-based TKH scheme for massive institution sizes.

Moreover, the entire computational overheads on the responder aspect for each protocols remain almost steady no matter the dimensions of the multicast institution. Protocol 2 outperforms protocol 1 with a factor of just about two with respect to computation, a aspect of virtually 3 with admire to transmission, and a set quantity of 11.3 µJ for reception energy.1 The whole computation strength for protocol 12 is about 238 mJ and for protocol 23 it's miles 119 mJ. considering that with two Zinc-carbon AA batteries of one.5 V nominal voltage and 800 mAh common capability, the available energy4 is 8640 J. Therefore, these values correspond to zero.0027% of the overall available strength for one complete execution of protocol 1, and zero.0017% of that of protocol 2. Taking most effective the execution of those protocols into account, it implies that protocol 2 (i.e., on the responder side) can execute the key settlement round 57600 times, while protocol 1 can execute 1/2 of it.

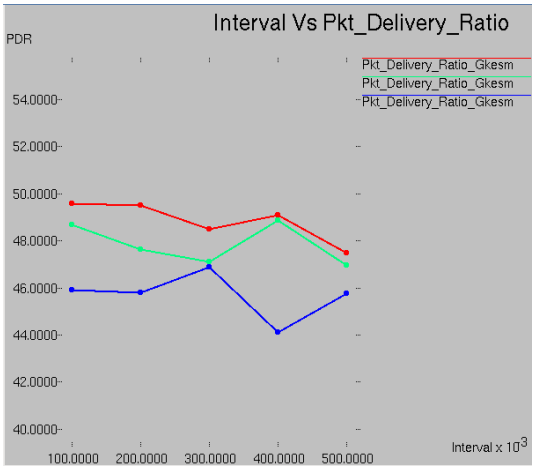

Fig. 1. Interval vs Packet delivery ratio

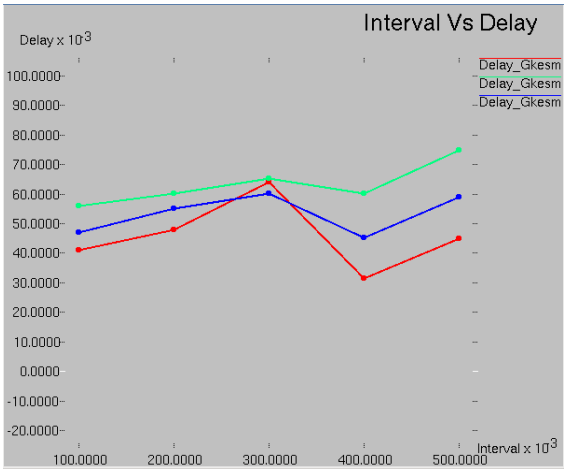

Fig.2. Interval vs Delay

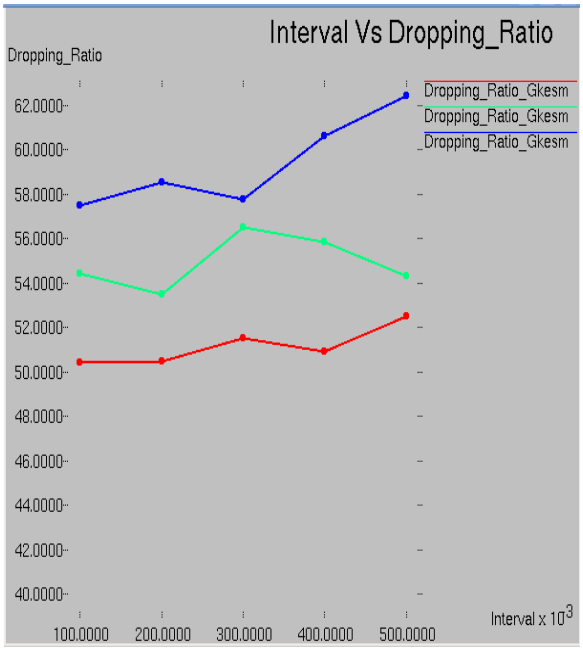

Fig.3. Interval vs Dropping Ratio

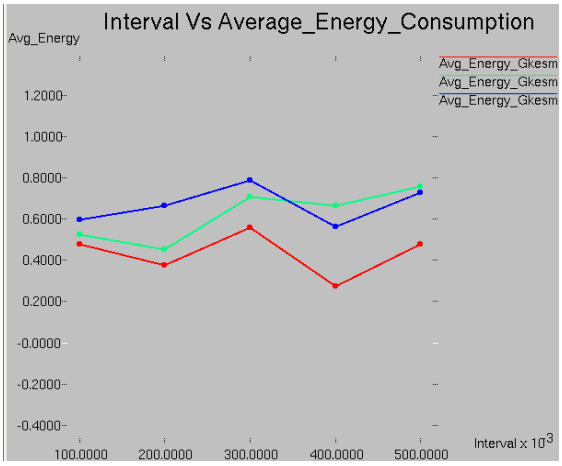

Fig.4. Interval vs Average Energy Consumption

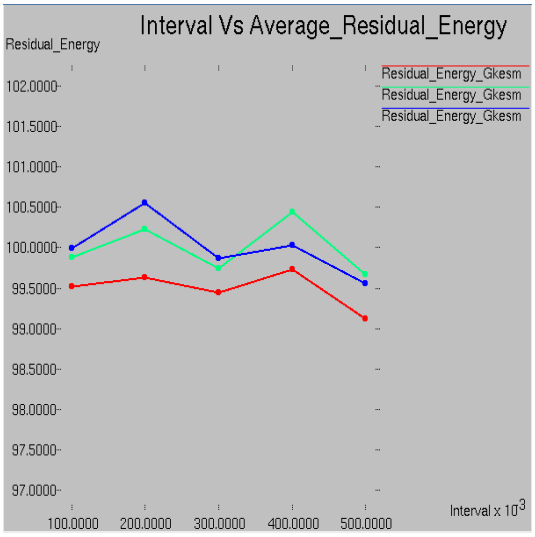

Fig.5. Interval vs Average Residual Energy

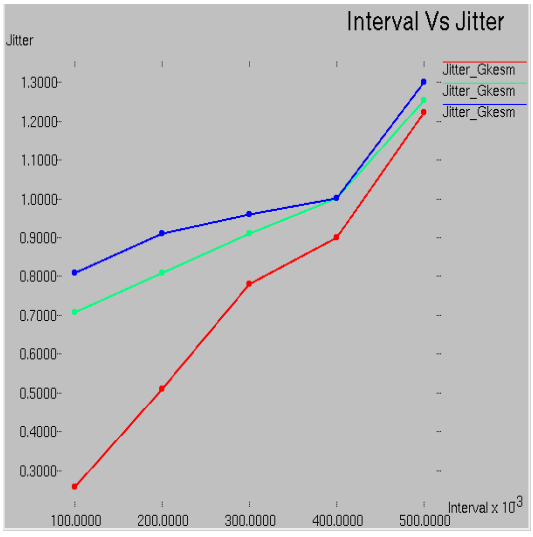

Fig.6. Interval vs Jitter

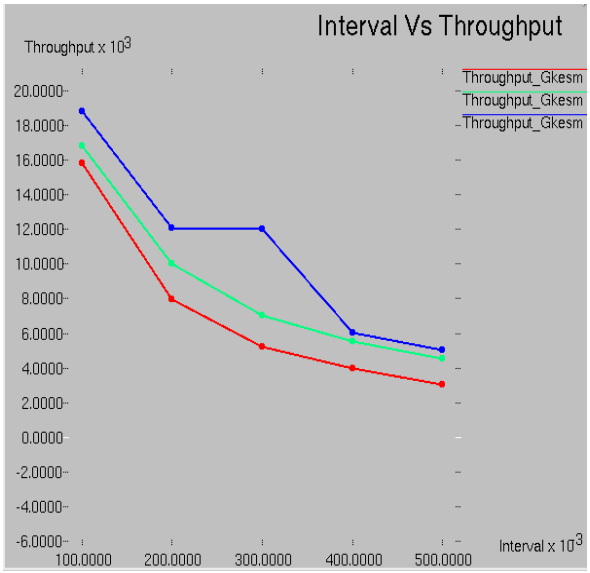

Fig.7. Interval vs Throughput

IV. CONCLUSION

This paper designed and analyzed two comfortable institution key establishment mechanisms for multicasting in WSNs inside the context of IoT programs. The key derivations also implicitly authenticate institution participants, while the key may be similarly used for securing multicast messages.

In step with the performance reviews consequences, computation and communication strength consumptions of each protocols are tolerable via the useful resource-constrained sensor nodes. The safety analysis measures the more powerful safety capabilities of these protocols proposed in comparison to reference solutions. Scalability residences of those protocols ensure the aid of common adjustments of the multicast group. Even though the fact that scalability and safety characteristics are closely coupled with both protocols, protocol 2 always outperforms protocol 1 in phrases of power intake. Protocol 1 is greater appropriate for IoT programs, which require group contributors to notably make a contribution to the important thing computation and need greater randomness. For the reason that power cost at the responder side is very low, protocol 2 is greater appropriate for centralized IoT packages, in which mostly cryptographic operations are done by means of a valuable entity and side nodes have very low strength profiles. The two protocols proposed are relevant to 1-to-many (1 : n) conversation eventualities and they're anticipated to be extended to many-to-many (m : n) communication scenarios obtaining comprehensive quantitative results for actual-time test-beds.

REFERENCES

[1] P. Porambage, C. Schmitt, P. Kumar, A.Gurtov, and M. Ylianttila, ‘‘Two- phase authentication protocol for wireless sensor networks in distributed IoT applications,’’ Apr. 2014, pp.

[2] P. Nie, J. Vähä-Herttua, T. Aura, and A. Gurtov,‘‘Performance analysis of HIP Diet exchange for WSN security establishment,’’Wireless Mobile Netw., 2011, pp.

[3] V. Shoup. (2001). A Proposal for an ISO Standard for Public Key Encryp-tion (Version 2.0). [Online].

[4] National Institute of Standards and Technology.(Aug. 1999).Recom-mended Elliptic Curves for Federal Government Use. [Online].

[5] J.-H. Son, J.-S. Lee, and S.-W. Seo,‘‘Topological key hierarchy for energy- efficient group key management in wireless sensor networks,’’ Wireless Pers. Commun., vol. 52, no. 2, pp. 359– 382, 2010.

[6] 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. [Online].

[7] Rahman and E. Dijk. (Oct. 2014). Group Communication for the Constrained Application Protocol (CoAP). [Online].

[8] J. Zhang and V. Varadharajan, ‘‘Wireless sensor network key management surveyand taxonomy,’’ J. Netw. Comput. Appl., vol. 33, no. 2, pp. 63–75, 2010.

[9] W. Yuan, L. Hu, H. Li, and J. Chu, ‘‘Security and improvement of an authenticated group key transfer protocol based on secret sharing,’’Appl.Math. Inf. Sci., vol. 7, no. 5, pp. 1943–1949, 2013.

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

[11] P. Porambage, C. Schmitt, P. Kumar, A. Gurtov, and M. Ylianttila, ‘‘PAuthKey: A pervasive authentication protocol and key establishment scheme for wireless sensor networks in distributed IoT applications,’’ Int. J. Distrib. Sensor Netw., vol. 2014, Jul. 2014.

[12] D. Hankerson, A. J. Menezes, and S.Vanstone, Guide to Elliptic Curve Cryptography. New York, NY, USA: Springer-Verlag, 2003.