Lightweight Secure and Reliable Authentication for Cluster Based WSN

Sangamesh J. Kalyane, Nagaraj B.Patil

Abstract-Wireless sensor networks (WSNs) are distributed all over the globe and are widely used for physical collection of data sensed in its surrounding. Tiny, affordable, constrained battery power, information processing capability devices called sensor nodes, plays a crucial role in agriculture, army, industry, intelligent grid, health care, critical infrastructure, etc. WSNs are often exposed to types of attacks. Once a sensor is affected by adversaries, the sensor's data materials become non- protective and intercepted by the enemy. In this paper we propose a lightweight polynomial secrete key (LWPK) sharing mechanism for secure hierarchal cluster based communication. LWPK is built on elliptical curve cryptography by exchanging symmetric keys to secure data transmission. Set of tests is carried on discrete event simulation tool and simulation results achieves better performance in terms of communication overhead, packet delivery ratio, end to end delay and network lifetime

Keywords: Key sharing, key pre distribution, security, wsn

I. INTRODUCTION

The Wireless Sensor Network (WSN) is a set of randomly or deterministically deployed small sensor nodes in a region of concern. These nodes can exchange information between them without using a pre-existing or centralized network infrastructure or control. Sensor nodes communicate to Base Station (BS) through single or multi hop transmission. The data is routed through intermediate nodes by routing protocol [1]. These routing protocols are classified into two categories: Flat and cluster based. Since sensor nodes are energy constrained, cluster based routing is effective way to improve the network lifetime than flat based routing [2]-[5]. In cluster routing, sensor nodes divided into set of groups or clusters. In each cluster one sensor node is selected as cluster head (CH) based on high residual energy and others as cluster members. CH has vital role in assisting its cluster members to route sensed data to sink or BS via single or multihop transmission.CH collects data from members, aggregates and transmits to BS. WSN is exposed to major security issues while routing data to its destination securing the data traffic is a challenging issue in cluster based routing [6]. Well-known LEACH [7] protocol has proven energy efficient routing for cluster; CH aggregates data and routes to BS.

Revised Manuscript Received on October 30, 2019.

Sangamesh J. Kalyane, Departmen t of CSE Bheemanna Khandre Institute of Technology Bhalki, India.

Dr. Nagaraj B. Patil, Principal, Govt Engg College Gangavati, India.

LEACH is vulnerable to malicious attacks, CH becomes compromise to malicious node and can launch attacks like spoofing, blackhole and crypto attacks that may disrupt the network. Thus LEACH has to be secured from malicious attacks to guarantee confidentiality, integrity, freshness and authentication of the originating node of the transmitted message. In this paper we propose lightweight cryptographic key exchange scheme using polynomial secrete sharing keys to ensure secure data transmissions in cluster based routing. Initially BS distributes polynomial secrete key shares k to CH, CH communicates to BS through inter cluster communication. CH aggregates data along with secrete key is forwarded to BS and keys are reconstructed at BS achieving secure communication.

The rest of this paper is organized as follows. In Section II describe the related work carried out. Section III describes the propose system model. In section IV the performance analysis and relative simulation are conducted. Finally we draw the conclusion on the proposed scheme in section V.

II. RELATED WORKS

Symmetric key cryptography provides better key management system for WSN; keys are distributed before node utilizes it. In [8-10] authors have come up with different pair wise key distribution techniques. In [11] author proposed random key distribution scheme, where the nodes selects randomly from keys subset generated by key generator and stores their keys along with their identities. This scheme could create a connected graph among two adjacent nodes and secure communication between them. If the keys are matched it would establish direct secure link and if mismatch captures the malicious node. In [12] author proposed low energy based key management for hierarchical WSN, network was divided into group of clusters comprising CH and cluster members. Shared secrete keys are stored in CH memory. Each cluster members selects key from CH and exchanges with CH along with sensed data. If the key matches with the CH memory it creates protected connection, if not matched CH requests intended secrete key from matching CH. However this scheme fails for large scale WSN. To resist sinkhole, selective forwarding and flooding attacks SLEACH [8] was proposed to secure hierarchal clustering using message authentication code (MAC) and detects intruder from becoming CH and injecting fake data. In [9] author proposed RLEACH, to improvise random pairwise key management. Since the LEACH was not able to resist malicious threats and shared keys was not properly shared to all adjacent nodes.

RLEACH could efficiently detect and resist Sybil and selective forwarding attacks.

III. SYSTEM MODEL PRELIMINARIES

Assumptions in modelling the network

- Sensor nodes are static after forming clusters
- BS assigns unique key and ID for each sensor nodes
- All sensor nodes has same transmission range

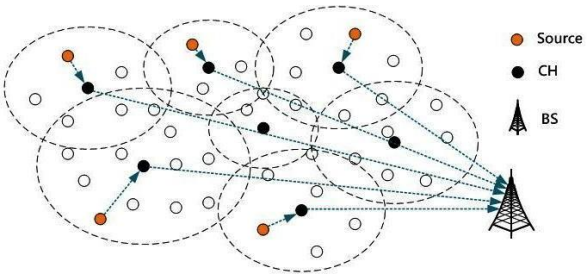

Figure 1: Network Model

Polynomials have two variables and their monomials is the sum of the indices of variable which is represented as

$$P \models x^i y^i$$

Bivariate polynomial of monomial degree $\deg(P) = i + j$ is

Symmetric keys are established between sensorS_i and cluster head is as follows:

- Sensor nodes broadcasts its ID's
- CH which is within the transmission range of sensor node S_i receives request and its ID, then sends key request message to BS
- BS looks up shared secrete key table for ID and picks corresponding key K_{S_i-CH}
- BS along with K_{S_i-CH} and $K_{CH-T_{BS}}$ and sends to CH
  along with $H(K_{S_i-CH})$
  $$E_n(K_{S_i-CH})_{K_{CH-T_{BS}}} \| H(K_{S_i-CH})$$
- CH decrypts message using $K_{CH-T_{BS}}$ to get K_{S_i-CH} for integrity check

Inter Cluster pairing keys

Inter-cluster pairing is done once the keys are pre-loaded into sensors once the sensors are authenticated inter cluster communication is established.
given as

- Two Cluster heads exchange their ID's CH_1

and CH_2

$$f(x,y) = \sum_{i,j=0}^{t} a_{ij} x^i y^j$$

According to large scale key distribution for WSN, for given polynomial of n variables the sensor nodes has shares of

- Each node evaluates stored polynomial secrete shares upon receiving ID's and generates

(ID_{CH_1}, ID_{CH_2})

$f(ID_{CH}, ID_{CH})$

secrete key k among $n-1$ variable and the polynomial degree
is t then sensor needs to store $(t+1)n-1$ coefficients of galois field $GF(q)$
Lagrange's interpolation is used to reconstruct secrete keys for polynomial degree k for $k+1$ points is given as

$$P_j(x_i) = yj \prod_{\substack{k=1 \\ k \neq j}}^{k+1} \frac{x_i - x_k}{x_j - x_k} \, mod\ N$$

- Polynomial $f(x,y)$ is symmetric then $(ID_{CH_1}, ID_{CH_2}) = f(ID_{CH_2}, ID_{CH_1})$

IV. SIMULATION RESULTS AND ANALYSIS

$x_j - x_k$

We evaluate our proposed scheme performance in terms of average energy consumption, computation delay, packet delivery ratio and transmission overhead. Simulation were

Proposed Lightweight mechanism

Key generation phase: The Base station (BS) T_{BS} selects random polynomial degree of $(x)\ of\ (t-1)$

$$(x) = S + a_1 x + \ldots\ldots + a_{t-1} x^{t-1}\ (mod\ n),$$

Where secrete$= (0)$, coefficients S, a_1, a_2, … . , $a_{t-1}$are finite with each nodes and BS computes shares $S_i = (x_i)$ for $\{i = 1, \ldots n\}$ then distributes $S_i$to each nodes under BS T_{BS}.

Using bitwise XOR keys are computed as

$$K_{S_i-CH} = k1 \oplus k2 \oplus k3$$

Sensor nodes S_i are pre-loaded with keys along with their ID's

At each levels by changing the threshold dynamically by using lagrange method for each level sensor node $i \in [1, m-1]$,
$\alpha_{i+1} = \alpha_i + \beta_i$ and finally α_m is calculated after calculating
$\{\alpha_1, \alpha_2, \alpha_3 \ldots \alpha_m\}$.

Intra cluster pairing keys

carried on discrete event tool, results were analysed and compared with existing group key management scheme. The disadvantage of group key scheme is, if group key is determined by the fixed formula, the adversary will obtain all previous and future keys by compromising nodes in the network. Table 1 show the simulation parameters and performance of proposed scheme is analysed.

Table 1: Simulation Parameters

Parameters	Value
MAC	802.11
Propagation Model	TwoRayGround
No of Nodes	80
Network Area	1000 x 1000
Simulation Time	100sec
Malicious Nodes	4
Initial Energy	10J
Antenna	Omni

Security Analysis

In our proposed scheme, even if the CH is compromised, the keys of the other sensor nodes are not revealed.
Compared to the group key scheme, if the CH is compromised the keys of the other nodes can be made available by computing the component key search within a key string. Our scheme provides strong tamper proof for CH which does not provide to retrieve keys when the attacker tries to retrieve keys by any act. Figure 2 shows the resilience of network successful rate when the nodes are attacked, proposed scheme performs better results compare to group scheme.

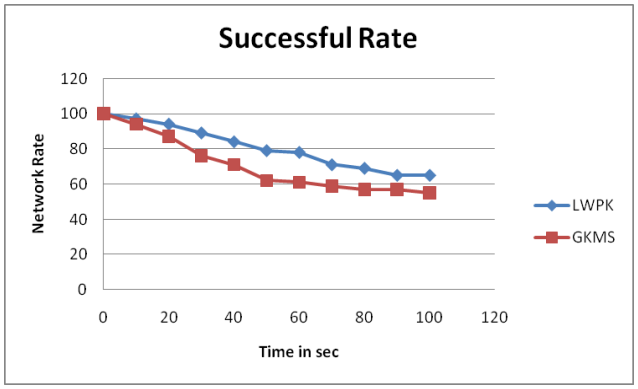

Figure 2: Network Successful Rate Energy Consumption and Computation Overhead

In figure 3 shows the average energy consumption of proposed scheme, the energy equation is given as

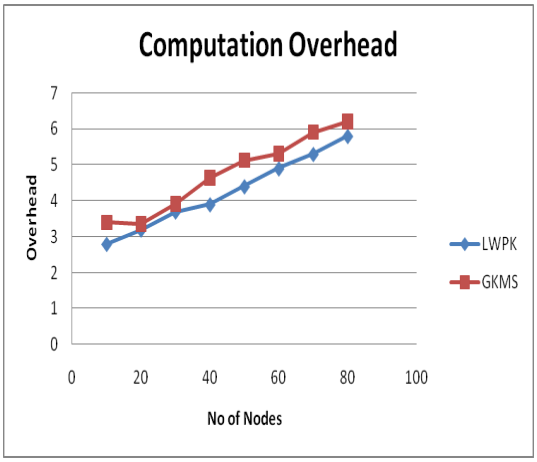

Figure 4: Computation Overhead Packet Delivery Ratio

Figure 5 shows the packet delivery ratio, it is seen that when the malicious activity in the network leads to packet drop. Our scheme has ability to prevent any malicious activity and reduces the packet drop ratio than group scheme. Here we introduce selective forward attack nodes and analyse its behaviour. In the presence of malicious nodes, any node sending packet which is not authenticated will be eliminated

$$Consumed$$
$$Energy\ used = Initial\ Energy$$
$$X\ 100\ \%$$

by the CH unless the keys of the sensor nodes are authenticated and CH will not establish communication between them until it is verified. In the below figure our
It is observed that our scheme consumes less power for key search than evaluating polynomial computation. The CH uses significant energy for computation due to intra cluster polynomial and utilises minimum energy of CH. Compared to group key scheme, CH consumes more energy in searching and authenticating keys of sensor nodes which does not extend network lifetime. We have also evaluated computation overhead in generating, authenticating, verifying keys. The proposed scheme has less overhead than group key scheme because of using symmetric keys for authentication. It will not allow attacker to compute polynomial component of keys if attacker tries any act. Figure 4 shows the computation overhead graph.

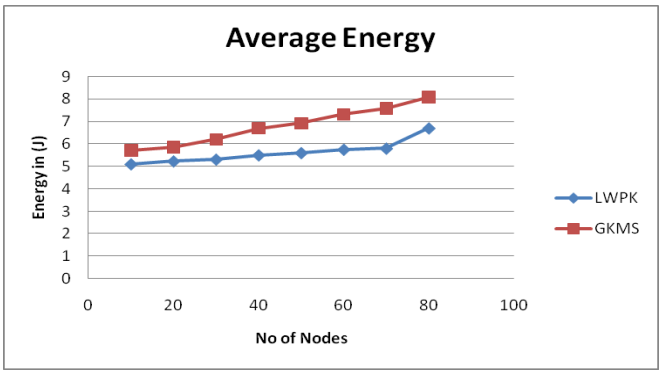

Figure 3: Average Energy Consumption

scheme achieves more PDR and delivers more authentic packets.

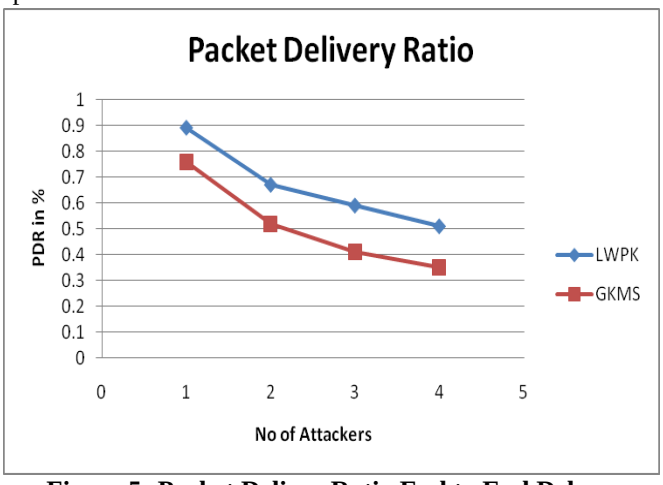

Figure 5: Packet Deliver Ratio End to End Delay

Figure 6 shows average end to end delay results, we observe the delay is less in our scheme compared to group scheme. We analyse delay in terms of cryptographic operation in generating and verifying keys. We note that time taken to generate keys for independent nodes are lesser.

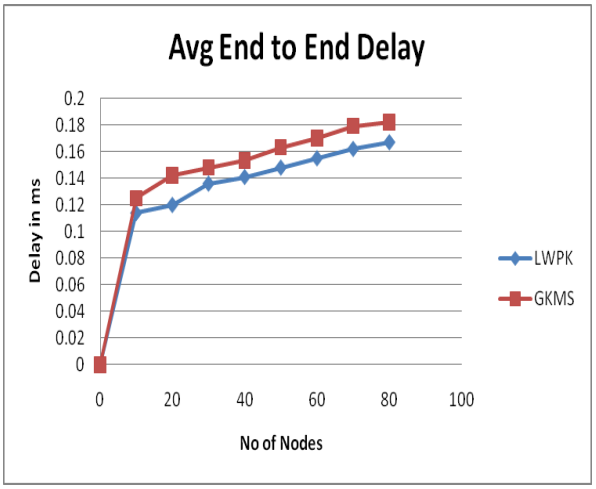

Figure 6: Average End to End Delay

V. CONCLUSION

In this paper we focus on providing lightweight key management scheme for hierarchal cluster based WSN. We propose a lightweight polynomial secrete key (LWPK) sharing mechanism for secure hierarchal cluster based communication. This scheme is based on ECC symmetric key exchange and establishes secure cluster communication. Proposed scheme ensures better security requirement and it can be robust again malicious attacks. We have compared our scheme with existing group key scheme and evaluated performance in terms of overhead, packet delivery ratio, end to end delay and energy consumption. Simulation results show our scheme out performs than group key scheme and it is energy efficient.

REFERENCES

1. J. N. Al-Karakki and A. E. Kamal, "Routing technique wireless sensor networks: a survey," *IEEE Wireless Communications*, vol. 11, no. 6, pp. 6–28, Dec 2004.
2. V. Katiyaar, N. Chand, and S. Soni, ``A survey on clustering algorithms for heterogeneous WSN," *Int. J. Adv. Netw. Appl.*, vol. 2, no. 4, pp. 745_754, 2011.
3. J. N. Al-Karakki and A. E. Kamal, ``Routing techniques in wireless sensor networks: A survey," *IEEE Wireless Commun.*, vol. 11, no. 6, pp. 6_28, Dec. 2004.
4. S. P. Singh and S. C. Sharama, ``A survey on cluster based routing protocols in wireless sensor networks," *Procedia Comput. Sci.*, vol. 45, pp. 687_695, 2015.
5. A. A. Abbassi and M. Younis, ``A survey on clustering algorithms for wireless sensor networks," *Comput. Commun.*, vol. 30, nos. 14_15, pp. 2826_2841, Oct. 2007
6. Z. J. Has, L. Yang, M.-L. Liuu, Q. Li, and F. Li, *Current Challenges and Approaches in Securing Communications for*
7. *Sensors and Actuators*. Springer Berlin Heidelberg, 2014, pp. 569–608.
8. W. R. Heinzeelman, A. Chandrakasan, and H. Balakrishnan, "Energyefficient communication protocol for wireless microsensor networks," in *Proceedings of the IEEE HICSS33*, Jan 2000, p. 10 pp. vol.2.
9. A. C. Ferreira, M. A. Vilaça, L. B. Oliveria, E. Haabib, H.
10. C. Wong, and A. A. Loureiro, *On the Security of Cluster- Based Communication Protocols for Wireless Sensor Networks*. Springer Berlin Heidelberg, 2005, pp. 449–458.
11. K. Zhang and C. Wang, "A secure routing protocol for cluster-based wireless sensor networks using group key management," in *4th IEEE International conference on WiCOM'08*, Oct 2008, pp. 1–5.
12. Blom, R. (1985). Proceedings of the EUROCRYPT 84 Workshop on Advances in Cryptology: Theory and Application of Cryptographic Techniques (pp. 335–338).
13. Duu, W., Deng, J., Haan, Y., & Varshney, P. (2003). A pairwise key pre-distribution scheme for wireless sensor networks. In Proceedings of the 10th ACM Conference on Computer and Communication Security-CCS '03 (pp. 42–51). doi:10.1145/948109.948118
14. Chan, H., & Perig, A. (2005). PIKE—Peer intermediaries for key establishment in sensor networks. In Proceedings IEEE 24th Annual Joint Conference of the IEEE Computer and Communications Societies (Vol. 1, pp. 524–535). doi:10.1109/infcom.2005.1497920.
15. Echenauer, L., & Gligor, V. (2002). A key-management scheme for distributed sensor networks. In Proceedings of the 9th ACM Conference on Computer and communications security-CCS '02, (pp.41–47). doi:10.1145/586110.586117.
16. Jolly, G., Kuscu, M., Kokatte, P., & Younis, M. (2003). A low-energy key management protocol for wireless sensor networks. In Proceedings of the Eighth IEEE Symposium on Computers and Communications ISCC(Vol.1,pp. 335–340). doi:10.1109/iscc.2003.1214142.

AUTHORS PROFILE

Mr. Sangamesh J.Kalayne Received the Bachelor's degree in Computer Science and Engineering from Visvesvaraya Technological University Belagavi, Karnataka 2002, M. Tech. degree in Computer Science and Engineering from JNTU Hyderabad, Aandra Pradesh in 2011. From April 2012 to till date working as an Assistant professor in Department of Computer Science and Engineering at Bheemanna Khandre Institute of Technology Bhalki- Karnataka.His research interests areas are ,Wireless Sensor Networks, Network Security , Computer Network and Management &presently pursing Ph.D under VTU, Belagavi, from 2015.

Dr. Nagaraj B. Patil Received the B.E. degree from The University of Gulbarga Karnataka 1993, M. Tech. degree from the AAIDU University of Allahabad in 2005,and the Ph.D. degree from the University of Singhania Rajastan India in 2012.He is having teaching experience of 27 years including 7 years research, from 2010 to 2018 .He worked as a Associate professor and HOD Dept. of CSE & ISE at Government College of Engineering, Raichur Karnataka. Presently he is working as a Principal of Government Engineering College Gangavati Karnataka. His research interests areas are Image Processing and Wireless sensor network