ISSN (Online) : 2455 - 3662
SJIF Impact Factor :5.148

EPRA International Journal of Multidisciplinary Research

Monthly Peer Reviewed & Indexed
International Online Journal

Volume: 5 Issue: 5 May 2019

Published By :EPRA Publishing

EPRA International Journal of
Multidisciplinary Research (IJMR) *Peer Reviewed Journal*

ENERGY-EFFICIENT CLUSTER PROTOCOL FOR MAKING A SECURED DATA-TRANSMISSION ON WIRELESS SENSOR NETWORKS

P. Chitralingappa
Research Scholar,
Department of Computer Science and Technology,
Sri Krishnadevaray University,
Ananthapuramu,
Andhra Pradesh,
India

Dr. V. Raghunatha Reddy
Assistant Professor,
Department of Computer Science and Technology.
Sri Krishnadevaray University,
Ananthapuramu,
Andhra Pradesh,
India

ABSTRACT

On Wireless sensor Networks, Data Transmission and Data Integrity are prominent attributes which leads to a critical issue. Clustering is an influential and emphasized feasible factor to enhance the performance of WSN System. Data aggregation is a paramount topic and an adapt technique in diminishing the energy consumption of sensor-nodes on WSN's for yielding secure and an effectual big data-aggregation. Cluster heads gathered data from the cluster members and send it to the base station. But the data easily be conceded (compromised) by a massive attack. These attacks are more damaging if the CH is corrupted by a malicious node playing CH role. We proposed an Energy-Efficient Cluster Protocol for making a secured Data-Transmission on WSN (EECP-SDT). EECP-SDT is built on a combination of Elliptic Curve Diffie-Hellman key agreement protocol for secrete key generation and Hash Message Authentication Code (HMAC) for data integrity. We have evaluated the performance of EECP-SDT by simulation and performs comparisons with existing algorithms in terms of various parameters like Average Energy Consumption, Average Residual Energy, No of Nodes Alive and No. of Cluster Head Elected. The resultant simulation not only prolong the lifetime of wireless sensor networks, but also enhance routing security evidently.

KEYWORDS: *Clustered WSN,Aggregator-Signature; Data-Integrity; Diffie-Hellman;*

I. INTRODUCTION

Actually Sensor nodes are as usually resource oriented and power based on WSN's and they would always get retrained to storage and processing reources and they utterly differnt from traditional based networks. Basically WSN's must have their inherent resource constraints and desigining limitations and restrictions which are Low-Bandwidth, short Communication range, limited amount of energy and processing and storage at every SN (sensor-node). Data-Aggregation technique being considered as a Holy-Grail to diminish the energy consumption for WSN's. So still the technique has the inherent security issues which means attacks, data forge/alteration and data tamperings etc.Thus, being designed a secure and efficient data-aggreagtion methods are so paramount for Wsn's. Wireless Sensor Networks (WSNs), with a large number of cheap, small and highly constrained sensor nodes sense the physical world [1], has very broad application prospects [2] both in military and civilian usage, including military target tracking and surveillance [3], animal habitats monitoring [4], biomedical health monitoring [5] [6], critical facilities tracking [7]. Due to the remarkable advantages, comprehensive attention has been devoted to WSNs [8], and a number of schemes have been presented [9] [10] [11] [12] [13].

In 1984, Shamir introduced the identity-based (ID-based) cryptography [14], which eases the key management problem by eliminating public key certificates. In an ID-based cryptography, the user's public key is easily generated from this user's any unique identity information (e.g. the serial number, a mobile phone number, an email address, etc), which is assumed to be publicly known. A trusted third party, called the private key generator, generates and issues secretly the corresponding private keys for all users using a master secret key. Therefore, in an Identity-Based AS (Aggregate-Signature), verification algorithm only involves the signature pair, some public parameters and the identity information of signer, without using an additional certificate.

In 2003, Boneh et al. introduced an Aggregation-signature-scheme that compresses multiple signatures created by various users on various messages into a single-short aggreagate signature.The aggregate-signature's validity will be equvalent to the validity of each signature that uses to create the Aggregate-Signature. Whereby, the aggreagate-signature's validity, if and only if an every individual signer obviously signed on its original message with respectively. And combining the highlights of aggregate signature scheme and ID-based cryptography, we give an Identity-Based AS (Aggregate-Signature) scheme for WSNs in cluster-based method. The adversary in our security model has the capability to launch any coalition attacks.

The rest of the paper is prepared as follows. In the following section, we introduce some related work about aggregate signature schemes. In section II, overview of secure clustering algorithms and attack, In section III, System Model And Security Model, Section IV provides the Energy Efficient Cluster Formation Protocol for secure data transmission in Wireless Sensor Networks, In section V, simulation and results, Finally, Section VI is the conclusions.

II. OVERVIEW OF SECURE CLUSTERING ALGORITHMS AND ATTACKS IN WSN

Cluster topology is a very prominent one in wsn. At this topolgy, the BS which gatherd data from various sensor nodes and it will be the accessed point where the end-user can access the data which collected by it. It is a fixed one which is a farther one from their nodes. Actually, the BS would not have any constraints as compared to rest of nodes in the topology and it maintains large volume of data and processing the data and it can be acted as a huge repository. And from each and every cluster, one of the node selects as CH which plays a gateway among those sensor nodes and the BS.

The CH accomplishing all kind of functionalities which holds among the sensor nodes and the BS, the operations should be like passing instructions to the Cluster members and accumalating the data before passing it to the BS. In some cases it should be the SINK for the cluster nodes and BS will be the SINK for the CH's. Upon a cluster topology the member node sends and receives the data to and from its CH. The CH's of various Clusters should communicate among themselves for passing the data to the BS.

A. SECURE CLUSTERING ALGORITHMS

Basically in all clustering methods security and reliabiity phases of clustering and selection of CH have been drawn a good modesty attention so far. On the one hand, there are so many papers which surveys the security solutions applied on wireless sensor networks, e.g. [18], [19], [20], [21], [22], [23], [24]. These papers detail the common security issues in sensor networks, such as authentication, intrusion detection, secure routing, secure data aggregation, etc. However, none of these papers address the issue of secure building and data transmission in particular.

On the other side, some papers, e.g. [25], [26], handle the puzzle of secure clustering and secure CH selection at sensor networks which being focused on issues like dynamic key change, complexity, cluster head election criteria, and so on. Regrettably, the latter papers could not consider the security routing aspects of clustering [23]. By the proposed criteria we probed the existing secure clustering algorithms for WSN since its so easy to validate them.

SLEACH

A familiar LEACH Protocol is a secured version that built by the aid of SLEACH. SLEACH should avert an intruder node to pass a falsified data messages and stops sink-hole,selective-forwarding and Hello-Flooding attacks.But it never guarantees its confientiality and availabilty.

SS-LEACH

SS-LEACH is another one which delivers securitry and its so energy effectual/potent. It enhances the network capacity by progressing the patterns of selecting CH's and builds dynamic multipaths CH's chains to passing the data to the BS.

ESODR

In ESODR, the computational complexity would low and got good efficiency and scalability but it bother from the dynamic clustering nature of the network. In addition, it needs more memory sizing capcity to store both the encryption key and the hash digest.

SecLEACH

SSecLEACH is an improvement flake of SLEACH. It is a protocol for securing node-to-node communication on LEACH- based networks. It introduces symmetric key and one-way hash chain to yield different performance numbers on efficiency and security depends on its various parameter values.

RLEACH

LEACH is attempting to apply random pairwise key (RPK) scheme/ formula by RLEACH. RLEACH must have the stature to defend the attacks such as selective forwarding, sybil and hello flooding.

B. ATTACKS IN WSN

Attacks towards WSN can be classified into the following categories [27][28][29]:

1. External attacks vs. Internal attacks

The Node which ever attacks the network meant to be it never belongs to concern network and it would not have autgorization of network for accessing the sources. But there is a possibilty the internal node gives interanal attacks. It is the most powerful attack which causes destructions for functioning in sensor networks so defending methods/isms need to fight against it.

2. Passive attacks vs. Active attacks

Sans any detection the passive attacks will accumulate the data. Generally the attacker would have a ambit to hark the traffic exchanged among WSN nodes. Not withstanding at active attcks attcker tampers, replays or blocks arrived data.

3. Physical attacks vs. Remote attacks

C. AUTHENTICATION ALGORITHMS

Actually WS Nodes will be used for remote places and living areas to watch enviromental and physical conditions and current situations for concern areas. By this reason WSN prone to attcks so to hold communication, authentication of network is needed. Following are the authentication algorithms for wireless sensor networks[31].

RSA ALGORITHM

RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman who discussed the algorithm in 1977. This system will be used for encrypting the To generate the public key we use the equation : Q=d*P [33].

where d= any number selected within the range of (1 to n-1).

P is the point on the curve.[33]

n is the maximum limit (always a prime number).

ECC parameters are:

1. Key size- It uses small key size.[33][6]
2. Memory- low memory usage.[32][33]
3. Transmission- low transmission requirements.[33]

HASH ALGORITHM

A hash algorithm is derived as a function that transform/pass the data numeric value into a string of fixed length. Algorithm holds of rounds of hash function. Each and Every round receives/takes the input combination of recent messages/data block and output of the last round. Such procedure will be processed as many times as needed to hash the complete message. Hashes are widely utilized to notice if any changes are performed/accomplished in data objects[30][35]. Typical hash algorithms which have MD5, SHA-1, and SHA-256.[34].

Message Digest (MD5)

MD stands for Message Digest. MD5 hash algorithm is being widely used. It embeds the one-way hash function for the converting the data , providing the

At Physical attacks an attcker can physically propagate the sensor node that can be botherd through the falsified and distracted/devastated of the sensor hardware. But in some cases the remote attcks will be held at distantly.

4. Mote-class attacks vs. Laptop-class attacks

At Most-Class Attack the machine of attack will have an Equivalent natufre of material as sensor nodes that should be hacked.Not withstanding at Lap-Top-Class attacks the opponent utilizes of the device which is so magnificient with an enhanced source like Processing Power, Energy reserving, transmission power.

5. Attacks against routing

At WSN, Routing Protocol being gone through by cyber attacks as its spoofed, altered, tampered data, Selective forwarding, Sinkhole, Wormhole, Sybil attack and Hello flood attack.

message sans needing the secret key at separately. RSA parameters are:

1. Key size- It uses massive key prime numbers.[33]

2. Memory- high reminiscence usage.[33]

ECC ALGORITHM

ECC stands for Elliptic Curve Cryptography. It is established through Victor Miller and Nil Koblits in 1985.[8] It is another ism/method for executing public key cryptography. Equation for ECC is $y^2 = x^3 + ax + b$. Key generation : here, we generate the public key (Q) and the private key (d) [32].

affirmation related to the integrity of transferred file. It uses of 128-bit hash function[34]. By the natufre of transformation , original message is infeasible to calculate/quantify from the message digest. It can be used with authentication header (AH), internet key exchange (IKE). As of now it is not at use, due to collision were found in 2004.[12]

Secure Hash Algorithm (SHA-1)

SHA stands for Secure Hash Algorithm. Mostly used hash function is SHA-1 and it is the strongest algorithm rather than MD5 [30]. It uses of input of 264-bit in-length and affords 160-bit message digest[34].

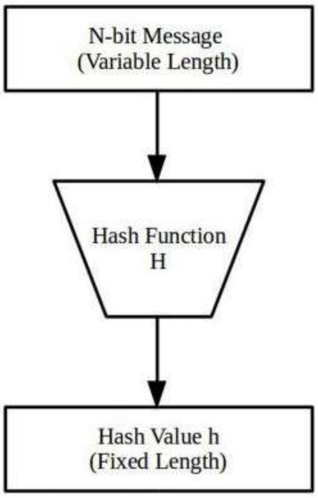

Fig-1: Hash Function

III. SYSTEM MODEL AND SECURITY MODEL

A. SYSTEM MODEL

Importantly, Security requirements on WSNs are confidentiality, integrity, authenticity, availability and Non-repudiation , etc. And actually the Data-Aggregation scheme for WSNs, it is paramount that no Data-Falisification for the during transmissions. So we prominently focus on the Data-Integrity safety at our system. The indispensable consideration of our system model is to gaurd the Data-Integrity whilst reducing bandwidth and storage cost for WSNs. Our Proposed system consists of three parts : Data Center, aggregator and sensor node.

DATA CENTER

Data center has a robust computing electricity and storage space. So it can process all original huge data collected by sensor nodes belong to the data center, and can provide the received information to consumers.

AGGREGATOR

Aggregator is a distinctive sensor node with positive potential to calculation and communication range. It can messages collecting from the physical world, process collecting data and forword to the base station.

SENSOR NODE

Sensor node has restrained resources in phrases of computation, memory and battery power. In our system, every sensor node belongs to one cluster, sends messages to their aggregator, and the messages will finally be despatched to data center through aggregator.

B. Mathematical Model of Identity-Based AS (Aggregate-Signature)

1. Sensor Network.
   Sensor network consisting of N sensor.
2. Neighbor.
   For any node whose neighbor node set are defined as follows:
   $Vi= \{i\in N|d\ (Vi,\ Vj) \leq R,\ n\neq i\}$,
   Where,
   N – No. of nodes
   d (Vi, Vj) the distance between node Vi, and Vj, R - Broadcasting range of nodes.
3. The energy spent for transmission of a k-bit packet over distance d is:

$$
\begin{aligned}
E_{Tx}(k, d) &= k * E_{elec} + k * \varepsilon_{fs} * d^2 \quad d< d_0 \quad (1)\\
&= k * E_{elec} + k * \varepsilon_{mp} * d^4 \quad d>= d_0 \quad (2)
\end{aligned}
$$

Where,

E_{elec} - base energy required to run the transmitter or receiver circuitry

ε_{fs} & ε_{mp} – Energy of the transmitter amplifier To receive the message energy required is

$$E_{RX}(k)=k*E_{elec} \quad (3)$$

4. Elliptical Curve Diffie-Hellman signature scheme is used to generate shared secret key for signing purpose and it has following parameters (CURVE, a, b, G, n, h).

Here,

CURVE – The elliptical curve
a and b are random numbers
G – Elliptical curve base point, a generator of the elliptical curve with large prime order n.
n – Integer order of G
h-cofactor

4.1 Key Generation

Sensor node creates a key pair, Private key integer d_A, randomly selected in the interval [1, n-1] and public key curve point $Q_A = d_A. G$.

4.2. Signature generation algorithm

4.2.1 calculate kA as randomly [myRand 1 [expr $N-1]]
4.2.2 xA= kA*Gx and yA =kA*Gy
4.2.3 r=xAmodN
4.2.4apply Cryptographic hash function and calculate s value
4.2.5 calculate hA and s=(r*dA*hA+kA)%N
4.2.6 The signature is the pair(r,s)

5. Node Registration
5.1 BS Assigns unique id for all nodes
5.2 Public/ private key generationand also
5.3 Generate Public/Private keys for all nodes
5.4 BS Generates inidividual key for all nodes
5.5 Partial Private/Public key

6. Pairwise Key Generation

Hash Message Authentication Code used for data integrity. One of the HMAC technique is Message Digest 5 (MD5) algorithm used for message integrity and calculating all pairs and generate public and private keys for all the nodes with other nodes in network simulation area.

7. Cluster Formation
7.1 Cluster Key Generation
7.2 Cluster Members Acknowledgement
7.3 Cluster Key Update

8. If any Cluster Head and Cluster Member is acting as malicious node discad its communication.
If (CH==Malicious node)
then leave that node and remaing members of that Cluster head are joined into its

neighbour cluster which is having more residual energy.

Else

Cluster member is acting as a malicious node simply dicard the node

9. Report Send to BS and BS send ACK msg to CH then Data is Collected from Cluster members and send to CH.

10. CH aggregate collected data and aggregated Data is Transmit to the BS.

IV. Energy-Efficient Cluster Protocol for making a secured Data-Transmission on WSN

In this section the proposed protocol, Energy-Efficient Cluster Protocol for making a secured Data-Transmission on WSN is explained. This concept is based on a mixture of two approaches: the primary one is the Elliptic Curve Diffie-Hellman key agreement protocol for secrete key exchange and the second one is the HMAC. To explain our proposal, a set of assumptions are specified as follows.

- ✓ The studied place is a WSN, in which sensor nodes are homogeneous in terms of process capacity, communication, energy and storage.
- ✓ However, BS is assumed to possess a limitless resource capability, trustworthy and answerable for the configuration of the nodes before the WSN deployment.
- ✓ In this study, an attacker is supposed to be passive or active throughout the operation of the network. BS and therefore the sensor nodes are now not mobile.

A. An Overview of Proposed Algorithm

The proposed protocol works based on the following pairwise keys: (i) shared between base station and cluster head (ii) shared between cluster head and cluster participants which form the same cluster. These keys are solely used for secure/impenetrable communications throughout the steady-state phase, both between BS and CH or between the CH and the member node. In fact, the keys are placed dynamically in the course of the Configuration phase. For safety reasons, the keys are renewed at evey round. However the establishment of these keys in the proposed protocol depends soley on ECDH.

The proposed protocol performs in three phases. The first one is initialization phase in which every sensor node SN is preloaded with a keys alongside with its pairs. In other words, this key will be used during the Configuration phase for the round 0. It is shared between all deployed nodes and BS. Generally, the global key is used for encrypting messages (for example, the broadcast message sent by BS to announce a new round) or to compute a HMAC. As a security measure, this key is renewed during the formation of clusters in the next phase. In the second phase (i.e. Configuration phase), the CHs are elected and clusters are formed where each CH broadcasts an announcement to neighboring nodes inviting them to be participants of its cluster in a secure/invulnerable manner. Thus, the pairwise keys are generated at some stage in this phase. The final phase is the steady-state phase in which data accumulated through the single nodes is transmitted to CHs which will in their turns forward them to BS. We point out that only the two final phases (i.e. Configuration phase and Stable-state phase) are repeated at every round. In Proposed algorithm, the messages exchanged are encrypted, and consequently the confidentiality of messages is assured.

B. Detailed description steps for Proposed Protocol

The Proposed algorithm is divided into three phases, namely:

1. Initialization phase

This phase is ensured with the aid of BS. During this phase, BS generates unique id for all nodes using a keyed one-way hash function H, and stores them at its level. BS generates ECC key pairs for each sensor node in the network, then it generates its ECC key pair for base station and also Each node is preloaded by ECC key pair. BS selects a key out of the set S, and then preloads it in all sensor nodes. After the WSN deployment, every node in the network can use this key to encrypt and decrypt messages exchanged or to calculate a HMAC. Note that the key can be regarded as a global key that will be used during the Configuration phase of the round p.

2. Configuration phase

This phase begins with the announcement of a new round via BS. By the three parameters such as distance from BS, residual energy and concentration. I should select the CH with the assistance /aid of Fuzzy logic mechanism. Only legitimate / professional nodes that have key, can decrypt and verify the validity of the HMAC. Once a simple node turns into CH, then this node encrypts CH identity , generates a HMAC and sends this data to BS. When BS receives the message of CH and if the HMAC is valid, the CH and BS establish the key using ECDH. After that, the CH encrypts a notification message adv and generates a HMAC by using a key. Then, it broadcasts this data and its CH public key to the set of nodes. The node receives the notification message, and soley the legitimate node that can decrypt adv, and decides his belonging to a cluster. Next, this legitimate node sends an encrypted message join_req and its node public key to CH chosen to inform of this decision. When CH receives the message join_req and if the HMAC is valid, the member node and CH establish the key pair. After the clusters formation, BS sends to each CH global key of the subsequent round. Each CH creates a TDMA schedule and sends to each member node a time slot course of which it can transmit its data. Thus, the CH sends the global key of the subsequent round. However, the time slots and the global key for the subsequent round are encrypted by the key pair CH and Cluster member.

3. Stable-state phase

During this phase, a member node sends to its CH data containing the captured value, in an encrypted manner. The collects data from all individuals of the cluster and transmits to BS after aggregation. BS decrypts the data and verifies the validity of the HMAC, in the advantageous case it accepts the aggregated data, otherwise it refuses this data.

V. SIMULATION AND RESULTS

Simulation of the WSN and its performance evaluation of following parameters have diagnosed and developed on NS2. The sensor nodes have been deployed randomly in a sensor-field in the range of 1000 ×1000 sqm.

- Average Residual Energy
- No of Nodes Alive.
- No of Cluster Head Elected.
- Average Energy Consumption

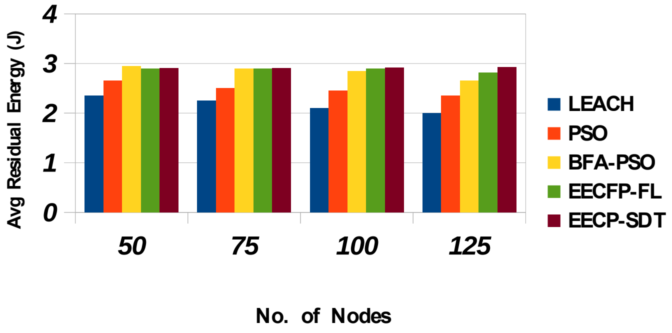

Fig-2: No. of nodes Vs Average Residual Energy

In the above Fig-2, Average Residual Energy, as deployed and enhancement of every 25 nodes EECP-SDT is showing better performance when compared with existing protocols are getting diminished.

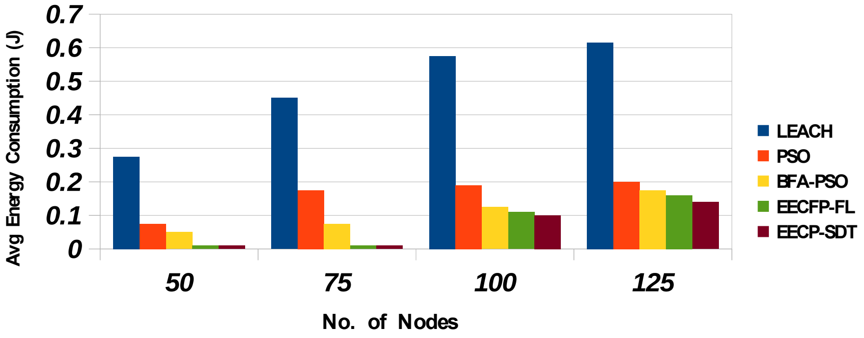

Fig-3: No. of nodes Vs Average Energy Consumption

In the above Fig-3, Average Energy Consumption, as deployed and enhancement of every 25 nodes EECP-SDT is showing better performance when compared with existing protocols are getting increased.

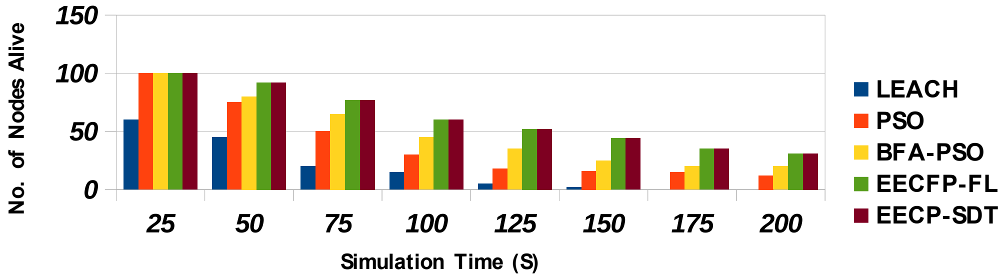

Fig-4: No. of Nodes Alive Vs Simulation Time

In the above Fig-4, No. of Nodes Alive with respect to the Simulation Time. For the increase in simulation time, total number of nodes alive in EECP-SDT is higher than that of existing algorithms which results in long span of network lifetime.

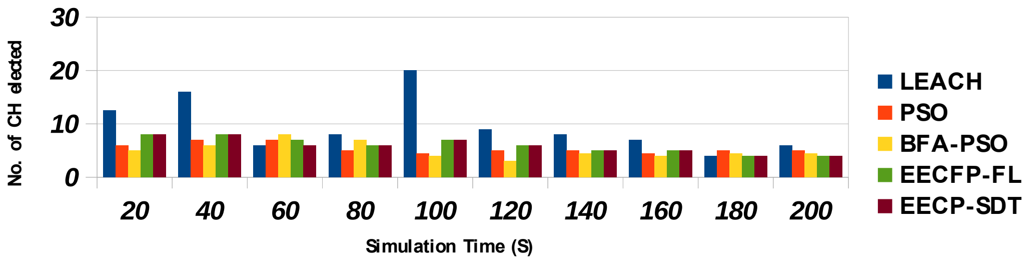

Fig-5: No. of CHs elected Vs Simulation Time

In the above Fig-5, the No. of cluster heads elected with respect to the simulation time. The proposed EECP-SDT produces more stable number of cluster heads with long alive nodes than the existing algorithms.

VI. CONCLUSION AND FUTURE ENHANCEMENT

In this paper, we have focused on the security of cluster- based routing protocols for WSN by proposing an Energy-Efficient-Cluster Formation Protocol for securing Data-Transmission on WSN (EECP-SDT). The proposed protocol is based on a combination of two main approaches; the primary one is the Elliptic Curve Diffie-Hellman (ECDH) key agreement protocol for generation of shared secrete and the second one is the HMAC approach for data integrity. The proposed protocol improves the security when compared with the earlier protocols which ensure only basic security requirements. Proposed one is robust against attacks compared with existing protocol. Its so worthy and valuable to note that proposed method would less the energy consumption in WSN's. We have evaluated the performance of EECP-SDT by using NS2 simulator and compared with an existing algorithms in terms of Average Energy consumption, Average Residual Energy, No. of Nodes Alive and No. of Cluster Head Elected. And further futuristic augments of my protocol targets to diminish the energy consumption towards computation and it will be aimed to deal with the dynamic cyber-attacks by making EECP-SDT as a target defense system.

REFERENCES

1. *M. M. E. A. Mahmoud and X. Shen, "A cloud-based scheme for protecting source-location privacy against hotspot-locating attack in wireless sensor networks," IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 10, pp. 1805–1818, Oct. 2012.*
2. *I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," IEEE Commun. Mag., vol. 40, no. 8, pp. 102–114, Aug. 2002.*
3. *J. Yick, B. Mukherjee, and D. Ghosal, "Analysis of a prediction-based mobility adaptive tracking algorithm," in Proc. IEEE 2nd Int. Conf. Broadband Netw., Boston, MA, USA, 2005, pp. 753–760.*
4. *A. Mainwaring, D. Culler, J. Polastre, R. Szewczyk, and J. Anderson, "Wireless sensor networks for habitat monitoring," in Proc. WSNA, Atlanta, GA, USA, Sep. 2002, pp. 88–97.*
5. *X. Lin, R. Lu, X. Shen, Y. Nemoto, and N. Kato, "SAGE: A strong privacy-preserving scheme against global eavesdropping for eHealth systems," IEEE J. Sel. Areas Commun., vol. 27, no.4, pp. 365–378, May 2009.*
6. *R. Lu, X. Lin, and X. Shen, "SPOC: A secure and privacy-preserving opportunistic computing framework for*

mobile-healthcare emergency," IEEE Trans. Parallel Distrib. Syst., vol. 24, no.3, pp. 614–624, Mar. 2013.

7. *N. Xu et al., "A wireless sensor network for structural monitoring," in Proc. ACM Conf. Embedded Netw. Sensor Syst., Baltimore, MD, USA, Nov. 2004, pp. 13–24.*
8. *J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey," Comput. Netw., vol. 52, no. 12, pp. 2292–2330, 2008.*
9. *N. Pereira, R. Gomes, B. Andersson, and E. Tovar, "Efficient aggregate computations in large-scale dense WSN," in Proc. 15th IEEE Real Time Embedded Technol. Appl. Symp. (RTAS), San Francisco, CA, USA, 2009, pp. 317–326.*
10. *X. Liu, H. Zhu, J. Ma, Q. Li, and J. Xiong, "Efficient attribute based sequential aggregate signature for wireless sensor networks," Int. J. Sensor Netw., vol. 16, no. 3, pp. 172–184, 2014.*
11. *]Y. Zhang, L. Sun, H. Song, and X. Cao, "Ubiquitous WSN for health-care: Recent advances and future prospects," IEEE Internet Things J., vol. 1, no. 4, pp. 311–318, Aug. 2014.*
12. *M. Rezvani, A. Ignjatovic, E. Bertino, and S. Jha, "Secure data aggre- gation technique for wireless sensor networks in the presence of collusion attacks," IEEE Trans. Depend. Secure Comput., vol. 12, no. 1, pp. 98–110, Jan./Feb. 2015.*
13. *R. C. A. Alves, L. B. Gabriel, B. T. de Oliveira, C. B. Margi, and F. C. L. dos Santos, "Assisting physical (hydro) therapy with wireless sensors networks," IEEE Internet Things J., vol. 2, no. 2, pp. 113–120, Apr. 2015.*
14. *A. Shamir, "Identity-based cryptosystems and signature schemes," in Proc. CRYPTO, vo 196. Santa Barbara, CA, USA, 1984, pp. 47–53.*
15. *D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and verifiably encrypted signatures from bilinear maps," in Proc. Eurocrypt, Warsaw, Poland, 2003, pp. 416–432.*
16. *S. Kent, C. Lynn, J. Mikkelson, and K. Seo, "Secure border gateway protocol," IEEE J. Sel. Areas Commun., vol. 18, no. 4, pp. 582–592, Apr. 2000.*
17. *J.-L. Koning and D. Dubois, "Suitable properties for any electronic voting system," Artif. Intell. Law, vol. 14, no. 4, pp. 251–260, 2006.*
18. *I. Butun, S. Morgera, and R. Sankar. A survey of intrusion detection systems in wireless sensor networks. IEEE Communications Surveys and Tutorials, 16(1), 2014.*
19. *A. Diop, Y. Qi, Q. Wang, and S. Hussain. An advanced survey on secure energy efficient hierarchical routing protocols in wireless sensor networks. International Journal of Computer Science Issues, 10(1), 2013.*
20. *P. Schaffer, K. Farkas, A. HorvTh, T. Holczer, and L. ButtyN. Secure and reliable clustering in wireless sensor networks: A critical survey. The International Journal of Computer and Telecommunications Networking, 56(11):2726–2741, 2012.*
21. *M. Patel and A. Aggarwal. Security attacks in wireless sensor networks: A survey. In International Conference on Intelligent Systems and Signal Processing, pages 329–333, 2013.*
22. *B. Radhika, P. Raja, C. Joseph, and M. Reji. Node attribute behavior based intrusion detection in sensor networks. International Journal of Engineering and Technology, 5(5):3692–3698, 2013.*
23. *A. Salehi, M. Razzaque, P. Naraei, and A. Farrokhtala. Security in wireless sensor networks: Issues and challanges. In IEEE International Conference on Space Science and Communication, pages 356–360, 2013.*
24. *G. Wang, D. Kim, and G. Cho. A secure cluster formation scheme in wireless sensornetworks. International Journal of Distributed Sensor Networks, 2012, 2012.*
25. *H. Rifa-Pous and J. Herrera-Joancomart. A fair and secure cluster for- mation process for ad hocnetworks. Wireless Personal Communications, 56(3):625–636, 2011.*
26. *D. Wu, G. Hu, and G. Ni. Research and improve on secure routing protocols in wireless sensor networks. In Fourth IEEE International Conference on Circuits and Systems for Communications, pages 853– 856. IEEE, 2008.*
27. *C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," Ad Hoc Networks, vol. 1, no. 2, pp. 293–315, 2003, sensor Network Protocols and Applications.*
28. *D. Djenouri, L. Khelladi, and A. N. Badache, "A survey of security issues in mobile ad hoc and sensor networks," IEEE Communications Surveys Tutorials, vol. 7, no. 4, pp. 2–28, 2005.*
29. *A. Kellner, O. Alfandi, and D. Hogrefe., "A survey on measures for secure routing in wireless sensor networks," IJSNDC, vol. 1, 2012.*
30. *https://www.tutorialspoint.com/cryptography/cryptography_hash_functions.htm*
31. *https://www.juniper.net/documentation/en_US/junos/topics/concept/ipsec-authentication solutions.html*
32. *http://www.ijcsmc.com/docs/papers/June2013/V2I6201330.pdf*
33. *http://edge.cs.drexel.edu/regli/Classes/CS680/Papers/EC_prezentacio.pdf*
34. *Middle-East Journal of Scientific Research 23 (Sensing, Signal Processing and Security): 108-117, 2015 ISSN 1990-9233©IDOSI Publications, 2015 DOI: 10.5829/idosi.mejsr.2015.23.ssps.30*
35. *Ahmed Al-Riyami, Ning Zhang, and John Keane, "Impact of Hash Value Truncation on IDAnonymity in Wireless Sensor Networks," Ad Hoc Networks, Vol. 45, pp. 80-103, March2016.*