International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 23 Issue 9 – DECEMBER 2016.

A Secure and Efficient Way for Data Aggregation Using Advanced Diffie Hellman and Signature Scheme for Wireless Sensor Networks

Ningappa Uppal[#1] and Dr. Arun Biradar[*2]

[#] M.Tech, Department of CSE, East West Institute of Technology, Bengaluru,India

[*] Head of the Dept., Dept. of CSE, East West Institute of Technology, Bengaluru,India

***Abstract*— The network lifetime mainly affected by limited energy in the sensor nodes. To overcome from that situation wireless rechargeable sensor networks has studied from past few years. Mobile charger moves in the known environment to charge the sensor nodes. To enhance the energy in the sensor nodes can be done by constantly recharging the nodes by mobile charger. Managing secure and productive enormous information total strategies is extremely appealing in the field of remote sensor systems look into. In genuine settings, the remote sensor systems have been extensively connected, for example, target following and environment remote checking. In any case, information can be effectively bargained by an immeasurable of assaults, for example, information capture attempt and information altering, and so forth. In this paper, we for the most part concentrate on information honesty assurance, give a character based total mark plot with an assigned verifier for remote sensor systems. As indicated by the benefit of total marks, our plan can keep information uprightness, as well as can lessen data transfer capacity and capacity cost for remote sensor systems. Besides, the security of our personality based total mark plan is thoroughly introduced in view of the computational Diffie-Hellman suspicion in arbitrary prophet display.**

***Index Terms*— Head nodes, big data, wireless sensor network, aggregate signature, coalition attack**

I. Introduction

Wireless sensor networks (WSN), sometimes called wireless sensor and actuator networks (WSAN) are 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.

In sensor network very important aspect is the flow of data. It contains information which may be important for some application. So there should be a secure data transmission. But maintaining security is difficult for sensor nodes because they have limited energy and limited memory capacity. Reports are made from the data received from sensor nodes. These report must be authenticate and reach without modification to the Base station.WSN are used in many application like military, ecological and health related area. This application may be surrounded by harsh, neglected and often adversarial physical environment. So Secure and Efficient data transmission (SET) is necessary and is important issue in WSN.

In big data era, digital universe grows in stunning speed which is produced by emerging new services, such as social network, cloud computing and internet of things. Big data are gathered by omnipresent wireless sensor networks, aerial sensory technologies, software logs, information-sensing mobile devices, microphones, cameras, etc. And the wireless sensor network is one of the highly anticipated key contributors of the big data in the future networks. Wireless sensor networks (WSNs), with a large number of cheap, small and highly constrained sensor nodes sense the physical world, has very broad application prospects both in military and civilian usage, including military target tracking and surveillance, animal habitats monitoring, biomedical health monitoring, critical facilities tracking. It can be used in some hazard environments, such as in nuclear power plants. Due to the remarkable advantages, comprehensive attention has been devoted to WSNs, and a number of schemes have been presented.

In 1984, Shamir introduced the identity-based (ID-based) cryptography, 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 (PKG), generates and issues secretly the corresponding private keys for all users using a master secret key. Therefore, in an ID-based signature (IBS) system, 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 aggregate signature scheme, which can compress multiple signatures generated by different users on different messages into a single short aggregate signature. The aggregate signature's validity can be equivalent to the validity of every signature which is used to generate the aggregate signature. That is to say, the aggregate signature is validity if and only if each individual signer really signed its original message, respectively. Hence, aggregation is useful technique in reducing storage cost and bandwidth, and can be a decisive building block in some settings, such as data aggregation for WSNs, securing border gateway protocols and large scale electronic voting system, etc.

In this paper, combining the highlights of aggregate signature scheme and ID-based cryptography, we give an ID-based aggregate signature (IBAS) scheme for WSNs in cluster-based method (Fig. 1).

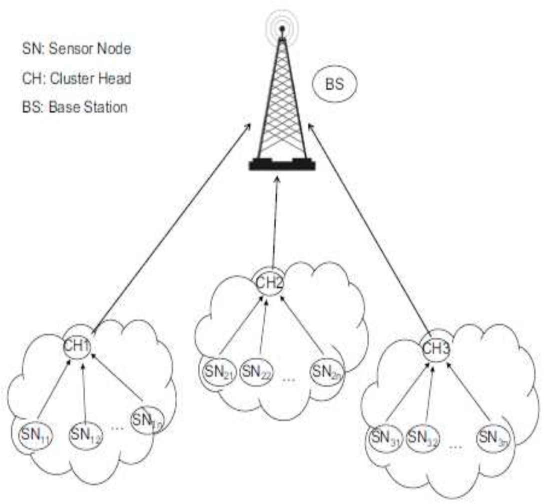

Fig 1. Cluster Based Network

The adversary in our security model has the capability to launch any oalition attacks. If an adversary can use some single signatures including invalid ones to generate a valid aggregate signature, we say that the attack is successful. In fact, our ID-based aggregate signature scheme not only can protect data integrity, but also can reduce bandwidth and storage cost for WSNs. The main contributions of this paper are fourfold.

II. Literature Survey

A. *Different Wireless recharging techniques*

Kurs *et al.*, [1] proposed in case of strongly coupled magnetic resonance one mobile charger travels in the environment to recharge energy to the sensor nodes, mainly magnetic resonance will work only when the distance is less between the sensor node and rechargeable magnetic resonance.

Alanson *et al.*, [2] have considered Battery free programmable RFID sensor device in Wireless identification and sensing platform (WISP).WISP functions in bidirectional communication channel and its wireless power comes in the range of few meters. But efficiency is less and freedom is more.

Shu *et al.*,[3] have proposed RFID-based wireless rechargeable sensor network to minimize the communication delay based on moving trajectory. The drawback is RFID Technology consumes more energy and packet transmission is slow.

B. *Single Mobile Chargers Protocol*

Peng *et al.*, [4] has presented, this algorithms recharges sensor nodes in more efficient manner when compared with other approaches. To increase the network lifetime, by mobile robot carrying the charger with enough energy. This system will properly when it identifying the bottleneck nodes to recharge.

Fu *et al.*, [5] have identified wireless rechargeable sensor network has the charging delay. Best conceivable development procedure of the charger, time to charge all nodes installed vitality stockpiling over an edge is minimized. Problem faced here RFID readers are very costly.

Ke *et al.*,[6] has been proposed Qi-Ferry(QiF) that physically holds energy and travels a WSN to wirelessly charge sensor batteries so as increase the network lifetime. Drawback of this Qi-Ferry is in which direction QiF should move and how many nodes it charges.

Angelopoulos *et al.*, [7] have studied very small amount of network information is used by distributed and adaptive protocols, to address three problems.

- At what extent all nodes should be charged.
- How the total energy is divided among the sensor nodes and mobile charger, and
- In which trajectory a mobile charger should move.

The main disadvantage of these protocols is that due to the limited information about the network .they will not work in larger network.

Haipeng Dai *et al.*, [8] studied Quality of Energy Provisioning (QoEP) upper and lower bounds for single and multiple origins. Every node has power capacity and power leakage is ignored.

He *et al.*, [9] considered an empirical recharge model based on experimental data .The energy provisioning has two forms of the problem one is point provisioning and path provisioning. Our deployment of nodes reduces the number of readers. Deployment plays very important role in the performance of the network.

Zi Li et al.,[10] considered J-RoC – a practical and efficient *J*oint *Ro*uting and *C*harging Scheme not only replenishing the sensor nodes but also improves network energy consumption rate and guides the routing activities in the network. Network lifetime can be increased. J-RoC works for single Mobile charger.

C. *Multiple Mobile Chargers Protocol*

Madhja *et al.* [11] identified usage of Multiple mobile charger is new way recharging to increase the lifetime of the network. Main tradeoff is how Mobile charger coordinates with each other and in which directions mobile charger should move.

Wang *et al.* [12] studied Multiple mobile chargers provide more scalability and robustness when compared with single mobile charger. Communication protocol used here is Named Data Networking (NDN).Tradeoff here is emergency charging.

Dai *et al.* [13] studied reducing the number mobile charger in the 2D network. Assuming uniform consumption of energy in all nodes, Assuming sensor nodes have constant energy depletion rate.Distance Constraint Vehicle Routing by reduction. drawback is when there is a non –uniform consumption of energy.

D. Simultaneous Wireless Charging

Liguang *et al.,* [14] have found that wireless charging vehicle charges multiple sensor nodes simultaneously. Advantage is it reduces number of power sources required in the network. Disadvantage is for longer distance poses more loss of the energy.

Shi et *al.,* [15] have investigated that energy is transferred to sensor nodes wirelessly in the efficient manner by

wireless charging vehicle. In order to increase the network lifetime, performance of charging will degrade when for longer distance between charger and node.

Liguang Xie *et al*.,[16] explore how scalability problem occurs in multi-node charging technology in a WSN. Because of that region Wireless charging vehicle (WCV) take a trip in the network in a timely fashion and charges the sensor nodes. On every trip WCV takes vacation then goes for next trip. They have used discretization and a novel Reformulation-Linearization Technique (RLT) to found the near optimal solution. But reformulating the non linear problem to linear one, the computational complexity is a major problem.

Cheng *et al.,* [17] considered the problem of jointly mobilizing the charger and scheduling sensor scheduling sensor nodes for charging distribution and optimal event capture nodes for efficient charging distribution and optimal event capture.

E. Collaborative Mobile Charging

Zhang et al.,[18], considered Quality of monitoring (QoM) problem in WRSN. Provides efficient charging distribution model to sensor nodes, scheduling is mainly faced here.

Zhao *et al.*,[19]Mobile charger can act as energy transfer to sensor nodes as well as a data collector to order increase network lifetime.

F. Mobile works as charger and data gathering

Songtao Guo et al.,[20]considered joint wireless energy replenishment problem and mobile data gathering for rechargeable sensor networks. In particular, SenCar have multi functionality they recharge the nodes and also gathers data from nearby nodes. There no procedure for forwarding the data to the sink.

[19],[21]-[22] Mobile charger serve for two purpose recharging and data gathering to enhance the network lifetime.

Yuanchao Shu et al [32] investigated Lifetime of Wireless Sensor Networks (WSNs) is less, because they have small batteries, and the inadequate energy supply is a major constraint. In Wireless energy transfer technology, broadcasting the electrical energy from a charger to sensor nodes, latest way of recharging the sensor nodes, to increase the network lifetime. But this technology is replaced by wireless rechargeable sensor networks (WRSNs) which have gained significance in the WSN research community. In WRSN, batteries in sensor nodes can be recharged by a mobile charger that sporadically travels in a known trajectory in the network. To increase the charged energy in sensor nodes, one problem is how to control the velocity of the charger.

III. System Approach

Most The main contributions of this paper are fourfold. First, we give the system models which have three components: data center, aggregator and a large number of sensor nodes. Aggregator works as a cluster head, can produce the aggregate signature and send it to the data center with the messages generated by the sensor nodes. Then, through a game played with a challenger and an adversary, the security model of identity-based aggregate signature schemes is introduced. And in the security model, the aggregation algorithm should resist all kinds of coalition attacks.

Second, we give a secure identity-based aggregate signature scheme for wireless sensor networks with a designated verifier (data center). Our scheme is composed of six probabilistic polynomial time (PPT) algorithms: Setup, Key Generation, Signing, Verification, Aggregation and Agg Verification.

Third, the detailed security proof is given based on the computational Diffie-Hellman assumption in random oracle model. The security proof indicates that our ID based aggregate signature scheme for wireless sensor networks can ensure the integrity of the data and reduce the communication and storage cost.

Fourth, through the analysis of comparative performance, we demonstrate that our identity-based aggregate signature scheme is efficient in terms of the communication and storage overhead.

A. System model

Security requirements in WSNs mainly are confidentiality, integrity, authenticity, scalability and flexibility, etc. In a data aggregation scheme for WSNs, it is important that no data falsify during transmissions. So we mainly focus on the data integrity protection in our system. The main consideration of our system model is to protect data integrity while reducing bandwidth and storage cost for WSNs. Our IBAS system consists of three parts: data center, aggregator and sensor node.

Data center has a strong computing power and storage space. So it can process all original big data collected by sensor nodes belong to the data center, and can provide the data information to consumers. At the beginning, every data center (as the designated verifier in our IBAS scheme) will receive its public-secret key. pair (PKcenter, SKcenter), and publish the public key PKcenter.

IV. OUR IDENTITY-BASED AGGREGATE SIGNATURE SCHEME

In this section, we provide a secure identity-based aggregate signature scheme. We adopt Sakai et al.'s signature scheme as the basis to construct our IBAS scheme. The scheme is described as follows.

Setup: Assume l is a security parameter, G1, G2 are two cyclic groups of prime order p. Let ^e : G1 × G1 → G2 be a bilinear pairing, and let P be an arbitrary generator of G1. H1, H2 and H are full-domain collision resistant hash functions. H1, H2: {0, 1} * → G1, H: G2 →Z* p. PKG chooses x, y ∈ Z∗ p randomly and computes P0 = xP, PKcenter = yP. Then the system parameters are param = {^e, G1, G2, P, p, H1, H2, H, P0}, the master secret key is msk = x. The data center's public-secret verification key pair is (PKcenter = yP, SKcenter = y). Key Generation: Given a sensor node's identity IDi, compute Qi = H1 (IDi) and the sensor node's corresponding private key is Si = xQi.

Signing: To sign a message mi, the sensor node IDi with the corresponding private key Si generates ti ∈ Z*p randomly, and computes Ti = tiP, hi = H2 (Ti, IDi, mi), Ui = Si + tihi. The signature is σ = (Ui, Ti, IDi, mi).

Verification: Given (σ, param), the verifier computes Qi = H1 (IDi) and hi = H2 (Ti, IDi, mi), then accepts if the following equation holds:

^e (Ui, P) = ^e (P0, Qi) ^e (Ti, hi).

Aggregation: Given an aggregate subset of sensor nodes belong to one cluster, each sensor node with the identity IDi provides a signature σi = (Ui, Ti, IDi, mi) on a message mi ∈ {0, 1}∗ of its collection, i = 1, • • • , n. Gained the data center's public key PKcenter from public channel, the aggregator computes

r = H (^e (U1, PKcenter), • • •, ^e (Un, PKcenter)), U = r • Σn i=1 Ui. σ = (U, T1, • • •, Tn) is the aggregate signature with identities {ID1, ID2… IDn} on messages {m1, m2, . . . , mn}, respectively.

AggVerification: Given an aggregate signature σ on the original messages mi ∈ {0, 1}* generated by the sensor nodes belong one cluster with the identity IDi, i = 1. . . n. The data center with public-secret key pair (PKcenter, SKcenter) computes Qi = H1 (IDi) and hi = H2 (Ti, IDi, mi).

V. DESIGN

Aggregator is a special sensor node with certain ability to calculation and communication range. It can sign messages collecting from the physical world, can get the data center's public key PKcenter from public channel, can generate the aggregate signature from the individual signatures signed by sensor nodes included aggregator itself, and can send the aggregate signature to the data center. We assume that the PKG generates the system parameters param; aggregator's private key SID corresponding to its identifier information ID, then embeds (param, SID) in aggregator when it is deployed.

Sensor node has limited resources in terms of computation, memory and battery power. We assume that the PKG generates private key SIDi for each sensor node IDi. When sensor node IDi is deployed, it is embedded with (param, SIDi). Every sensor node IDi can use its private key SIDi to sign messages collecting from the physical world. In our system, each sensor node belongs to one cluster, sends messages and its signatures to their aggregator, and the messages will finally be sent to data center via aggregator.

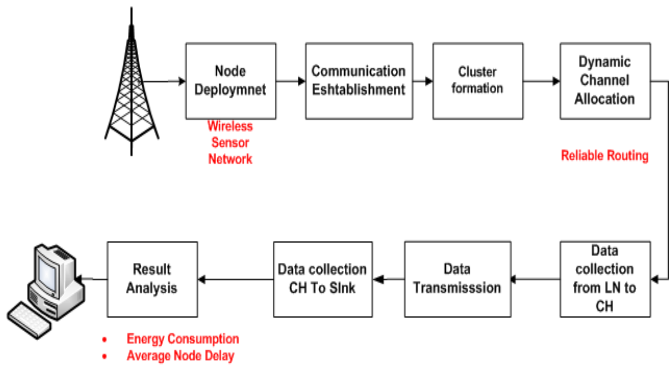

Fig 2. Proposed Architecture

An IBAS scheme is comprised of six PPT algorithms: Setup, Key Generation, Signing, Verification, Aggregation and AggVerification. Please refer to for the detailed instruction. Obviously, the goal of an adversary is the existential forgery of an aggregate signature. An IBAS scheme is secure if the basic signature scheme involved is existentially unforgivable against adaptive chosen message attacks (EUF-CMA secure), and the aggregation algorithm should stand up against all kinds of coalition attacks. Most of the former security models only consider the security of the basic signature scheme and the forgery of an aggregate signature, and do not consider the coalition attacks. So we mainly focus on the security of aggregation algorithm. When attacking the aggregation algorithm, the purpose of an adversary is to forge a valid aggregate signature while using some invalid individual signatures.

In the third phase, we consider the two dimensions Temporal Discretization and Spatial Discretization to discretize the velocity control. In Figure 3 Temporal Discretization shown a generic mobile charging scenario is considered, where the charger is mounted on a vehicle or a robot which may change its velocity. Considering the limited acceleration capability of a robot/vehicle, we discretized the charger's velocity. We present a discrete velocity model in which the charger's velocity can change only at discrete t=mΔt. where m∈N which remains constant between two adjacent discrete time instants.

$$|v_i - v_{i-1}| \le \alpha t_i \quad (6)$$

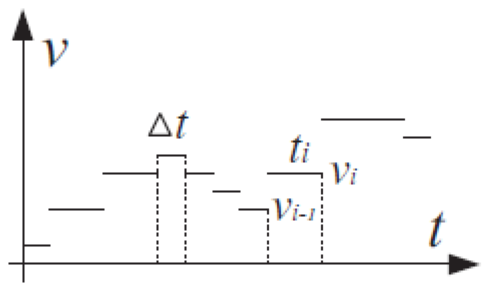

Fig 3 Discrete velocity

In Figure 4 Spatial Discretization is shown, we first determine the nearest and farthest points on the trajectory which have the highest and lowest charging power at the charging node j. Let Pmax j and Pmin j be the charging power at node j of these two points on the trajectory. To discretize the charging power at node j, we draw Rj concentric circles around j with an increasing radius. Specifically, given a small enough Discretization factor ε (ε > 0), the charging power between neighboring circles can be represented by a vector of discretized charging power Instead of calculating the charging power at different positions on the trajectory, we use the lower bound of the charging power of each segment, i.e., the charging power at positions on different circles.

To control the velocity with single node, the velocity control algorithm is used by taking discrete velocity & discretized trajectory as input and Control the velocity of charger.

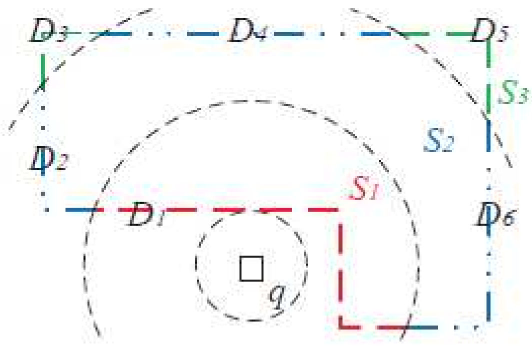

Fig 4 Trajectory discretization

Based on the velocity discretiztion and trajectory discretization. Designing the velocity control mechanism by assigning the patrolling cycle T_s to a different segments of the trajectory. Velocity control for the single node is stated as

$$\sum_{j=1}^{k} C_1^j\, t_j \qquad (7)$$

s.t

$$\sum t_j = T_s \qquad (8)$$

Algorithm 1: To control velocity for single node

Given Length,T_e,,α,є,n,k,C_j
Intialize the graph
for c = 1 to p-r+1 do
calculate $A_s(c,1)$
end for
for d = 1to r-2 do
for c = d to d + p-r do
for m = c+1 to d+p-r+1 do
calculate $E_s(m-c,d+1)$
for a = 1 to c-1 do
if a is true then
connect A_s (c,d) and A_s (c,d+1)
update A_s (c,d+1)=max(A_s $(c,d+1)_i$, A_s $(c,d)_r$ + E_s(m-c,d+1)
endif
end for
end for
end for
end for
for c= p-r to p-1 do
if a is true then
connect A_s(c,r-1) and A_s(p,r)
calculate E_s(p-c,r)
update A_s(p,r)
endif
end for
return A_s(p,r)

Phase 4 is scheduling and data collection. Scheduling method used here is Real time query scheduling(RTQS).In RTQS 1) The nonpreemptive query scheduler (NQS) achieves high capacity but cannot provide low response times to high-priority queries due to priority inversions. 2) The preemptive query scheduler (PQS) eliminates priority inversions at the cost of reduced capacity. 3) The slack stealing scheduler combines the advantages of preemptive and nonpreemptive schedulers to improve real time capacity while meeting query deadlines. And data collection is done by RREQ and RREP.Phase 5 includes the Recharging the sensor nodes.

Algorithm 2 :To control velocity for Multiple Nodes

Given Length,T_e,,α,є,n,q,C
Initialize the less charged energy E_{min} = 0
Discretize D_s based on v and t
for p = 1 to M do
Evaluate charging power
Calculate distance between the nodes by Euclidian distance
Get profile Rj run algorithm 1
Given Rj, Evaluate the energy charging E_{Rj} in all the nodes
if min E_{Rj} > E_{min} thenR_{min} = Rj
end if
end for
return R_{min}

VI. PERFORMANCE ANALYSIS

Graphs represent the performance of the proposed system in comparison with the previous works. Comparison is based on the following metrics:

Table 2 depicts the Network size, Number of nodes deployed, initial energy and Mobile charger.

TABLE 2 PARAMETERS OF SIMULATION AND VALUES

Simulation Parameter	Value
Node count	22
Initial energy	100 joules
Base station	0
Packet size	500
Routing protocol	DSR
Speed	200ms
Mobile node	200 joules

Fig 5 Average energy graph indicates the increase in energy when compared with existing system. Since our approach of recharging the head nodes, overcome problem of distance from mobile charger node to the sensor nodes. Increase in the average energy we can see that network lifetime is increased.

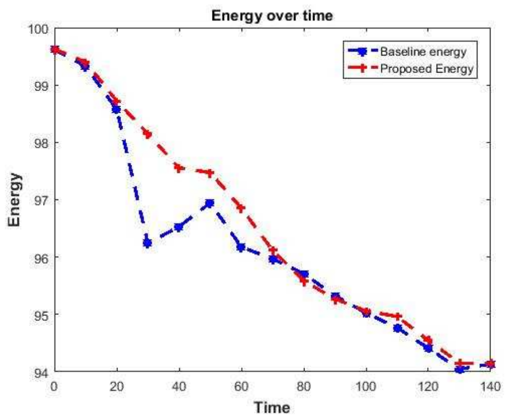

Fig 5 Average energy

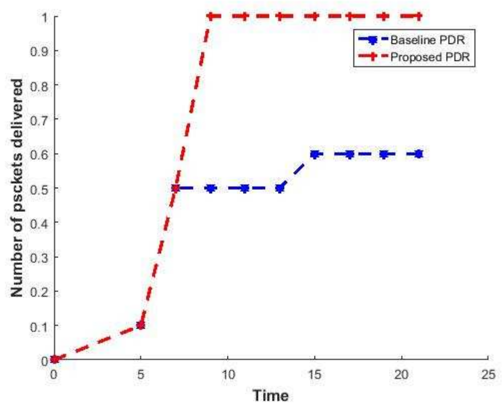

Fig 6 Packet delivery ratio

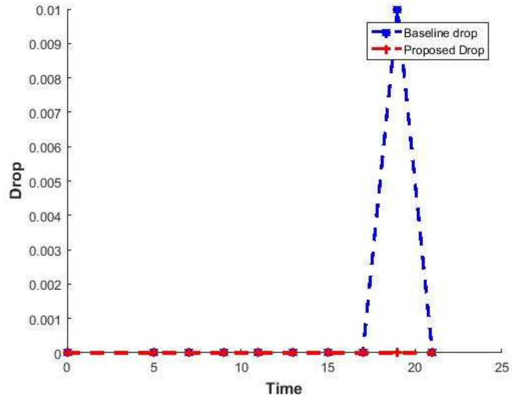

Fig 7 Packet Drop

Between 96 to 97 there is a drastic drop in energy in the existing system. When compared with proposed system less or minimum drop of energy.Fig 6 shows the graph of number packet delivered to destination correctly. Here existing system is compared with the proposed system. At 0.5 in the graph there is raise in the proposed. Fig 7 shows the packet drop in proposed system and existing system. When compared with existing system with proposed system. In 15 to 20 there is more packet drop in the existing system.

VII. CONCLUSION AND FUTURE WORKS

Wireless sensor networks are resource constrained where the energy efficiency is a major issue. Maximizing network lifetime, where the mobile charger moves in predefined known environment and charges the randomly deployed nodes in wireless rechargeable sensor networks. Mobile charger moves in the network to charge sensor nodes. The proposed approach achieves efficiency by reducing the velocity control and distance from the mobile charger to sensor nodes. Experimental results show that the minimum energy level is always maintained so that the network lifetime is maximized. we also have proved that our aggregate signature can resist coalition attacks, that is to say the aggregate signature is valid if and only if every single signature used in the aggregation is valid. In our future work, we will focus on designing more efficient data aggregation schemes.

Further the proposed approach can be applied in the feature work by adding more security by adding signature scheme and combining RSA and Diffie Hellman to enhance security features

ACKNOWLEDGMENT

The author would like to thank to Dr Arun Biradar HOD Dept of CSE, EWIT Bangalore,for providing encouragement, constant support and guidance which was of a great help to complete this research article.

REFERENCES

[1] A. Kurs, A. Karalis, R. Moffatt, J. D. Joannopoulos, P. Fisher, and M. Soljacic. Wireless power transfer via strongly coupled magnetic resonances. *Science*, 317:83–86, 2007.

[2] A..P. Sample, D. J. Yeager, P. S. Powledge, A. V. Mamishev, and J. R Smith. Design of an RFID-based battery- free programmable sensing platform. *IEEE Trans. Instrum. Meas.*, 57(11):2608–2615, 2008.

[3] Yuanchao Shu, Peng Cheng, Yu Gu, Jiming Chen, and Tian He. Minimizing communication delay in RFID-based wireless rechargeable sensor networks. In *IEEE SECON*, 2014.

[4] Y. Peng, Z. Li, W. Zhang, and D. Qiao. Prolonging sensor network lifetime through wireless charging. In *IEEE RTSS*, 2010.
[5] L. Fu, P. Cheng, Y. Gu, J. Chen, and T. He. Minimizing charging delay in wireless rechargeable sensor networks. In *IEEE INFOCOM*, 2013
[6] K. Li, H. Luan, and C. C. Shen. Qi-ferry: energy-constrained wireless charging in wireless sensor networks. In *IEEE WCNC*, 2012.
[7] Constantinos Marios Angelopoulos, Sotiris Nikoletseas, and Theofanis P. Raptis. Wireless energy transfer in sensor networks with adaptive, limited knowledge protocols. *Computer Networks*, 70:113–141, September 2014.
[8] H. Dai, L. Xu, X. Wu, C. Dong, and G. Chen. Impact of mobility on energy provisioning in wireless rechargeable sensor networks. In *IEEE WCNC*, 2013.
[9] S. He, J. Chen, F. Jiang, D.K.Y. Yau, G. Xing, and Y. Sun. Energy provisioning in wireless Rechargeable sensor networks. *IEEE Transactions on Mobile Computing*, 12(10):1931–1942, Oct 2013.
[10] Z. Li, Y. Peng, W. Zhang, and D. Qiao. J-RoC: a joint routing and charging scheme to prolong sensor network lifetime. In *IEEE ICNP*,2011.
[11] Adelina Madhja, Sotiris Nikoletseas, and Theofanis P. Raptis. Efficient, distributed coordination of multiple mobile chargers in sensor networks. In *ACM MSWiM*, pages 101–108, 2013.
[12] Cong Wang, Ji Li, Fan Ye, and Yuanyuan Yang. Multi-vehicle coordination for wireless energy replenishment in sensor networks. In *IEEE IPDPS*, 2013.
[13] Haipeng Dai, Xiaobing Wu, Guihai Chen, Lijie Xu, and Shan Lin. Minimizing the number of mobile
[14] An Efficient Merkle-Tree-Based Authentication Scheme for Smart Grid Hongwei Li, Member, IEEE, Rongxing Lu, Member, IEEE, Liang Zhou, Member, IEEE, Bo Yang, Member, IEEE, and Xuemin (Sherman) Shen, Fellow, IEEE.
[15] EPPDR: An Efficient Privacy-Preserving Demand Response Schemewith Adaptive Key Evolution in Smart Grid Hongwei Li, Member, IEEE, Xiaodong Lin, Senior Member, IEEE, Haomiao Yang, Member, IEEE, Xiaohui Liang, Student Member, IEEE, Rongxing Lu, Member, IEEE, and Xuemin (Sherman) Shen, Fellow, IEEE.
[16] Engineering Searchable Encryption of Mobile Cloud Networks: When Qoe Meets Qop Hongwei Li, Dongxiao Liu, Yuanshun Dai, and Tom H. Luan.
[17] Enabling Fine-grained Multi-keyword Search Supporting Classified Sub-dictionaries over Encrypted Cloud Data Hongwei Li, Member, IEEE, Yi Yang, Student Member, IEEE, Tom H. Luan, Member, IEEE, Xiaohui Liang, Student Member, IEEE, Liang Zhou, Member, IEEE, and Xuemin (Sherman) Shen, Fellow, IEEE.
[18] An Efficient Privacy-Preserving Outsourced Computation over Public Data Ximeng Liu, Member, IEEE, Baodong Qin, Robert H. Deng, Senior Member, IEEE, Yingjiu Li, Member, IEEE.
[19] Efficient and Privacy-Preserving Outsourced Calculation of Rational Numbers Ximeng Liu, Member, IEEE, Kim-Kwang Raymond Choo, Senior Member, IEEE, Robert H. Deng, Fellow, IEEE, Rongxing Lu, Senior Member, IEEE, and Jian Weng.