MAXIMIZING NETWORK LIFETIME USING HECC ALGORITHM FOR WIRELESS SENSOR NETWORK

C. Priyadarsini[1] Dr.R. Prema[2]

Abstract

A wireless sensor network is one among the thrust research area in wireless communication. Due to its sensing nature, it has been deployed in many application scenarios. The increasing technological advancements such as Internet of Things (IoT) and much more, wireless sensor networks pave the way for many research dimensions. Data aggregation is one among the research paradigm in such networks. Also there exists security thrusts when the communication medium is wide open in air. An adaptive Hyperelliptic curve cryptography technique is applied for maximizing network lifetime over the wireless channel. The proposed protocol is implemented using NS2.Hyper Elliptic Curve Cryptosystems (HECC) is proposed to decrease the bits and computational overhead for ciphertext.This system is more efficiency and security. The proposed technique has been compared with the existing mechanism.

Keywords : Wireless sensor networks, reactive routing, Hyperelliptic curve, cryptography, throughput, key generation, aggregation latency.

I. Introduction

Wireless sensor network has number of sensor nodes that arecollaboratively collect and connectedby wireless medium. The sensor node is furnished with the sensing devices, micro-processor, limited memory,wireless transmitter and batteries. Sensor nodes in the network collect information from the environment and send to the destination. These WSN are deployed in various areas which includes data gathering, remote monitoring,factory automation, smart home and security. Sensor node dispose of computing, sensing and organized itself in order to transmit particular data to the node through multiple path. The deployed sensor nodes arepowered by limited lifetime batteries, which arecomplicated to bereplaced or recharged. There exist certain resource constraints in WSNs such as short communication range, low bandwidth, limited processing/storage and in particular, the energy consumption. A sample wireless sensor network with routing nodes is shown in Figure 1.

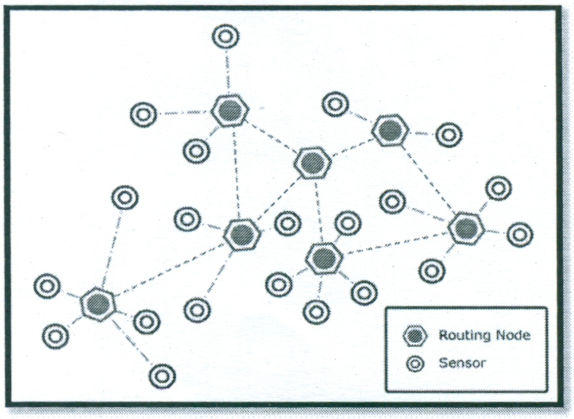


Figure 1. Wireless sensor network with routing nodes

[1]Research Scholar, Department of Electronics and Communication Systems, KarpagamUniversity, Karpagam Academy of Higher Education, Coimbatore, Tamil Nadu-641021 Phone : 8344521375

[2]Associate Professor, Department of Electronics and Communication Systems, Karpagam University, Karpagam Academy of Higher Education, Coimbatore, Tamil Nadu - 641021. Phone: 9345706892

Data aggregation is a basic ability of a wirelesssensor network (WSN). The common means of performing data aggregation is to have sensor nodes send their measurements to a particular node called a destination. Convergecast, is fundamental to WSNs. It build a logical tree known as convergecast tree underlying physical topology, data is routed to the sink along with the tree were sink is located nearer to the tree .In WSNs, as shown by Hill et al.[6], transmission of a single bit over a long distance consumes the same amount of energy as thousands of CPU instructions to exists. It reduce the communication overhead. This reduction increases the lifetime of sensor networks, another mechanisms, such as radio scheduling, control packet elimination, and topology control, help in reducing energy consumption, it is widely acknowledged approaches to reduce the energy consumption is in-network data aggregation [7–10]. Hence this paper aims to propose Secure Data Aggregation Routing Protocol (SDARP) for wireless sensor networks. The rest of the paper is organized as follows. The next section reviews the literatures. Section – 3 presents SDARP. Section – 4 portrays the simulation settings and performance metrics chosen in this research. Section – 5 depicts the results and discussions. Section - 6 concludes the paper.

II. Related Works

In recent years, the attention of researchers has been devoted to utilizing compressive sampling (CS) based data aggregation methods. To increase the network's lifetime by reducing the amount of data transmissions the Decentralized CS-based data aggregation method in used in WSNs.It simultaneously computes random measurements of the sensed data and transmit them throughout the network. The efficient Compressive Data Aggregation (CDA) method is to improve both cost and network's life-time in large-scale WSNs. In this the total data transmissions are decreased only when the number of required measured samples is small enough. Next method is an adaptive data aggregation method which applies CS on the local spatial correlation among data of neighboring sensor nodes it reconstruct data at the sink node. .

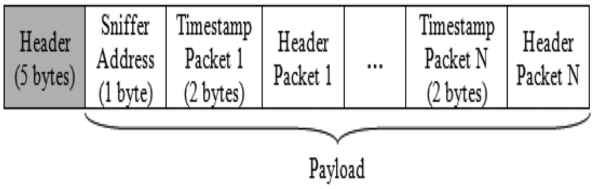
It is to be noted that in-network data aggregation reduces the redundant communication traffic, it is vulnerable to a wide range of attacks[11,12]. Adversaries / attackers can influence intermediate sensor node sand admittance the information stored in that [13–17]. Secure data aggregation protocols [18–31] aim at combining security and data aggregation together. Some of the data aggregation protocols with security implementation in the above literatures provide security in a hop-by-hop manner, where encryption and decryption operations are carried out at intermediate hops.. Therefore, the need to preserve the privacy of sensorreadings at intermediate nodes becomes imperative.

III. Proposed Framework

Data aggregation is one among the techniques in order to lessenthe congestion problem which is quite common in WSNs. Data aggregation will collect information from the nearby sensor nodes and then transmits only the useful informationto the end point. This results in lessening congestion. Among various types of data aggregation schemes, due the merits and demerits of the in-network and grid-based schemes,a hybrid approach basedon event duration and security aspect will be suitable enough to propose a protocol. The proposed Secure Data Aggregation Routing Protocol (SDARP)is a reactive protocol. The source sensor node will initiate data packet to sink node only after accomplishing route discovery. Also there will not be periodicalexchanges of routing information. Route discovery process in SDARP is done by making use of broadcasting route request (RREQ) packet. When a source

Sensor node is in need for a destination route for which it does not have a route already, it will then broadcast RREQ packet across the network. Destination sensor node receiving this packet will update the information for the source sensor node and sets up backward pointer information for the source node in the routing table. A lifetime is coupled with every reverse route entry. It is to be noted that when the route entry is not used within the lifetime it will be removed. Intermediate wireless sensor nodes will monitor the link status of next nodes in active routes. During a link break in an active route is detected, a route error (RERR) message is used to inform other sensor nodes that the loss of that link has occurred. The RERR message present in the proposed SDARP will mention the specific destination which is no longer reachable by way of the broken link.

The Diffie-Hellman algorithm with RSA requires a key of 1024 bits to achieve sufficient security. Also it is noteworthy that Diffie-Hellman algorithm based on ECC can achieve the same security level with only 160 bit key size. Hence in the proposed SDARP, hyperelliptic curve cryptography is applied for data aggregation. The packet format of SDARP is given below



3.1 Sender sensor node Authentication

Step 1: Sender sensor node registers with the base station sensor node which provide necessary details.

Step 2 : Base station node provides a sender sensor node id and a pair of keys, both public and the private key for HECC encryption for the newly registered sender sensor nodes and it is unique id . It stores the sender sensor node id along with its name in a database. Next time when the sender sensor node logins with his valid id, base station sensor node checks in the database whether the sender sensor node has registered already. If it is then sender sensor node is allowed to use base station sensor node services.

3.2 Data Encryption/Decryption

Data encryption and decryption is performed on sender sensor node side in this work to prevent information leakage of both its node data and key. This saves the resources in network by improving it efficiency.

Step 1: It encrypts data with public key provided by base station sensor node using hyper elliptic curve cryptography, before storing data in base station in sensor node.

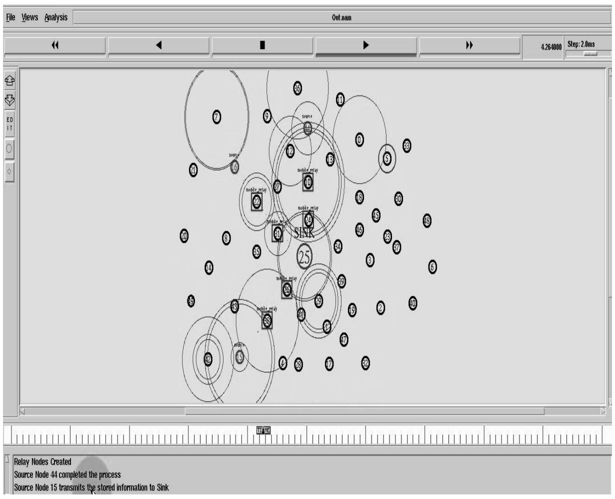
Step 2 : Encrypted data is decrypted by private key provided by base station,when it need data

IV. Simulation Settings And Performance Metrics

The NS-2 Simulator is used. The WSN nodes are placedrandomly between 500 and 1000. It transfer the packets at constant bit rate .Through GPS all the sensor nodes have the ability to communicate to their neighbor nodes and their own location information. The performance metrics chosen are Network lifetime. The simulation settings are depicted in Table 1. A sample simulation scenario using NS2 is shown in Figure 2.

Table 1. Simulation Settings

Parameter Name	Value
Nodes	500 nodes to 1000 nodes
Terrain Size	1500 meters X 1500 meters
Initial energy / node	50 joules
Processing time	1500 seconds
Power of Baseline node	6mW
Simulation runs	10
Packet size	300 bytes
Radio Propagation	Free Space
MAC Protocol	802.11
Radio Range	200 meters



Relay Nodes Created
Source Node 44 completed the process
Source Node 15 transmits the stored information to Sink

Figure 2. Simulation Scenario using NS2

V Results and Discussions

The performance metrics of network lifetime are chosen for simulation. The simulation is carried out with varying number of nodes ranging from 500 to 1000.The simulation result for number of nodes versus network lifetime is depicted in the Fig.3. From the results it is obvious that the proposed HECC achieves better performance in terms of network lifetime. The results are also presented in the Table2

Table 2 Number of Nodes VsNetwork Lifetime (seconds)

Number of Nodes	PDA [1]	MAI [2]	FASM [3]	SDARP
500	7048	7265	7402	7918
600	6892	7003	7284	7749
700	6774	6927	7109	7528
800	6511	6794	6901	7363
900	6381	6592	6729	7138
1000	6216	6301	6499	6920

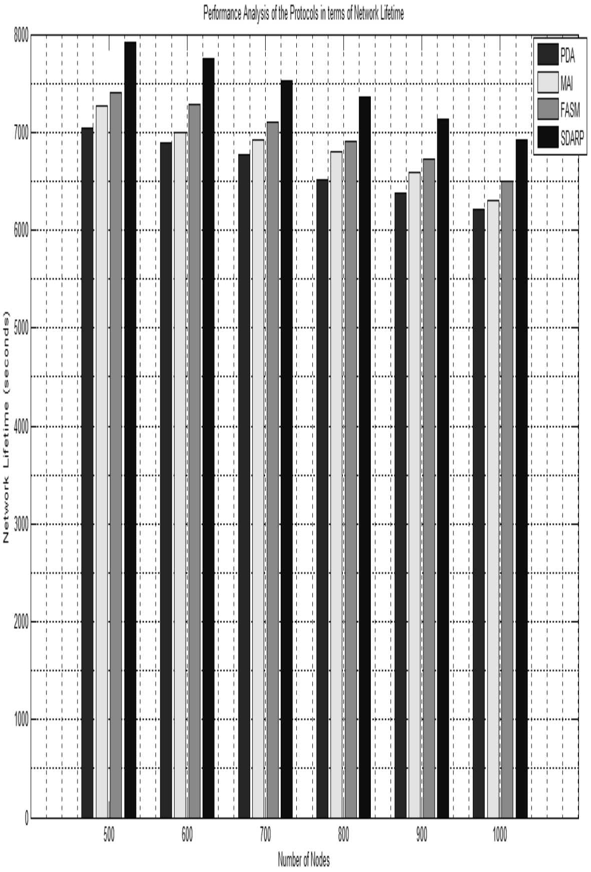


Figure 3. Number of Nodes Vs Network Lifetime (Seconds)

VI. Conclusions

The increasing technological advancements such as Internet of Things (IoT) and much more, pave the way for many research dimensions in wireless sensor networks. In this research work a Hyperelliptic curve cryptography technique is applied for increase network lifetime over the wireless channel. The proposed protocol is implemented using NS2.HECC is a fast public key cryptosystem with more efficiency and security. This paper intends to maintain data security by using HECC.

References

[1] S.Q. Ren, D.S. Kim, J.S. Park, A secure data aggregation scheme for wireless sensor networks, in: Proceedings of the Frontiers of High Performance Computing and Networking Workshops, ISPA, Lecture Notes in Computer Science,4743, Springer-Verlag, Niagara Falls, Canada, 2007, pp. 32–40.

[2] H. Yousefi, M. Malekimajd, M. Ashouri and A. Movaghar, *"Fast Aggregation Scheduling in Wireless Sensor Networks,"* in IEEE Transactions on Wireless Communications, vol. 14, no. 6, 2015, pp. 3402-3414.

[3] H. Li, K. Li, W. Qu, I. Stojmenovic, *"Secure and energy-efficient data aggregation with malicious aggregator identification in wireless sensor networks,"* Future Generation Computer Systems, Vol. 37, no.5, 2014, pp. 108-116.

[4] C. Luo, F. Wu, J. Sun, C.W. Chen, Efficient measurement generation andpervasive sparsity for compressive data gathering, IEEE Trans. Wirel.Commun. 9 (12) (2010) 3728–3738.

[5] J. Luo, L. Xiang, C. Rosenberg, Does compressed sensing improvethe throughput of wireless sensor networks? in : Proceedings of IEEEInternational Conference on Communications (ICC'10), 2010, pp. 1–6.

[6] J. Hill, R. Szewczyk, A. Woo, S. Hollar, D. Culler, K. Pister, System architecturedirections for networked sensors, ACM SIGPLAN Notic. 35 (11) (2000) 93–104.

[7] B. Krishnamachari, D. Estrin, S.B. Wicker, The impact of data aggregation inwireless sensor networks, in: Proceedings of the 22nd International Conference on Distributed Computing Systems, ICDCSW, IEEE, Vienna, Austria, 2002, pp. 575–578.

[8] A. Boulis, S. Ganeriwal, M.B. Srivastava, Aggregation in sensor networks: Anenergy-accuracy trade-off, Ad Hoc Netw. 1 (2-3) (2003) 317–331.

[9] R. Rajagopalan, P. Varshney, Data-aggregation techniques in sensor networks:A survey, IEEE Commun. Surveys Tutorials 8 (4) (2006) 48–63.

[10] E. Fasolo, M. Rossi, J. Widmer, M. Zorzi, In-network aggregation techniques forwireless sensor networks: A survey, Wireless Commun. 14 (2) (2007) 70–87.

[11] L. Hu, D. Evans, Secure aggregation for wireless networks, in: Proceedingsof the Symposium on Applications and the Internet Workshops, SAINT, IEEE,Washington, D.C., USA, 2003, pp. 384–391.

[12] B. Przydatek, D. Song, A. Perrig, SIA: secure information aggregation in sensornetworks, in: Proceedings of the 1st International Conference on EmbeddedNetworked Sensor Systems, SenSys, ACM, Los Angeles, USA, 2003, pp. 255–265.

[13] H. Chan, A. Perrig, Security and privacy in sensor networks, Computer 36 (10)(2003) 103–105.

[14] C. Karlof, D. Wagner, Secure routing in wireless sensor networks : attacksand countermeasures, Ad Hoc Netw. 1 (2-3) (2003) 293–315.

[15] Y. Wang, G. Attebury, B. Ramamurthy, A survey of security issues in wireless sensor networks, IEEE Commun. Surveys & Tutorials 8 (2) (2006) 2–23.

[16] A. Becher, Z. Benenson, M. Dornseif, Tampering with motes: real-world physical attacks on wireless sensor networks, in: Proceedings of the 3rd International Conference on Security in Pervasive Computing, SPC, Lecture Notesin Computer Science, 3934, Springer-Verlag, York, UK, 2006, pp. 104–118.

[17] X. Chen, K. Makki, K. Yen, N. Pissinou, Sensor network security : a survey, IEEECommun. Surveys & Tutorials 11 (2) (2009) 52–73.

[18] J. Girao, M. Schneider, D. Westhoff, CDA: concealed data aggregation in wireless sensor networks, in: Proceedings of the Workshop on Wireless Security,WiSe, ACM, Philadelphia, USA, 2004, pp. 1–2.

[19] D. Wagner, Resilient aggregation in sensor networks, in : Proceedings of the2nd Workshop on Security of Ad Hoc and Sensor Networks, SASN, ACM,Washington D.C., USA, 2004, pp. 78–87.

[20] J. Girao, D. Westhoff, M. Schneider, CDA : concealed data aggregation for reverse multicast traffic in wireless sensor networks, in: Proceedings of the40th International Conference on Communications, ICC, IEEE, Seoul, Korea, 2005, pp. 3044–3049.

[21] C. Castelluccia, E. Mykletun, G. Tsudik, Efficient aggregation of encrypted datain wireless sensor networks, in: Proceedings of the 2nd Annual InternationalConference on Mobile and Ubiquitous Systems: Networking and Services,MOBIQUITOUS, IEEE, Washington, D.C., USA, 2005, pp. 109–117.

Author's Biography

Dr. R. Prema is working as Associate Professor in the Department of Electronics and Communication Systems at Karpagam University. She has 13 years of experience in teaching. She has published 15 papers in the national and international journals and presented 14 papers in the national and international conferences.

C. Priyadarsini is Research Scholar in Departmentof Electronics and Communication Systems at Karpagam University .She has published 3 papers in the national and international journals and presented 2 papers in the national Conferences.