International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-2, December 2019

Energy Efficient and Secured Data Dissemination in Wsn

U.Nandhini, Santhosh Kumar SVN

Abstract*: Data dissemination is a high level application service, provided to WSN to update the configuration parameter to make the node perform intended services. The configuration parameters of the nodes are updated by means of reprogramming and reconfiguration through over air programming. In data dissemination, the data are so sensitive that even a small change in a data will lead to data corruption and nodes will not perform intended services. In most of the existing systems, providing energy efficient secured data dissemination is a major concern. The attackers can interrupt the process data dissemination and launch various types of attacks, In-order to overcome these challenges. In this paper, a novel Secure Based Dissemination protocol is proposed which can provide energy efficient data dissemination. The proposed protocol ensures better authentication during data dissemination. The proposed protocol is implemented in NS2 simulator. Simulation results justifies that, proposed protocol output forms the existing techniques and has better Packet Delivery Ratio, throughput , network life time, energy consumption, end to end delay and routing overhead .

***Keywords*: Wireless Sensor Network, Fitness Function, Energy Optimization, Life Time, Efficient Routing**

I. INTRODUCTION

WSN is a distributed collection of tiny sensor nodes which are deployed to sense the natural events in the environment. The sensed data are transmitted to Base Station (BS) and transmitted for the further processing. The nodes in WSN are self-organizing and they can establish the ad hoc network connection on the fly, regardless of how many number of nodes that are malfunctioned in the network. Another important feature of WSN is in network collaborative processing**.**

Data dissemination is a high level application and activity provided to WSN to update or reinstall the existing code in WSN. Through over air programming, the data dissemination in WSN is achieved by using two methods namely reconfiguration and reprogramming. Modifying the existing code from the scratch to change the entire behavior of the node is called as reprogramming. Normally Reprogramming in data dissemination for WSN is expansive in terms of communication and computation.

Revised Manuscript Received on December 30, 2019.
***** Correspondence Author
Santhosh Kumar SVN*, School of Information Technology and Engineering, VIT University, Vellore, India, santhoshkumar.svn@vit.ac.in
U.Nandhini M.Tech(Software Engineering),School of Information Technology and Engineering, VIT University, Vellore, India, nandhinin071@gmail.com

Transmitting few bytes of data for the purpose of updation in the node behavior is called as reconfiguration. Comparing reconfiguration with reprogramming, reconfiguration is preferred. Since data transmitted in reconfiguration is fewer compared with reprogramming. In data dissemination security is a major concern. Data transmitted using data dissemination is very sensitive. Thereby even a small change will lead to corruption of entire data, the nodes fails to perform intended services. The most of existing data dissemination protocols are vulnerable to various security attacks. Motivated from all these observations, in this paper a novel data dissemination which can be able to provide better optimized energy efficiency with better security is proposed in this paper.

II. LITERATURE SURVEY

There are various works proposed by the various authors for the energy efficient secured data dissemination protocols. Among them Neeraj Kumar et.al [1] have proposed a Secure and Energy Efficient Data Dissemination protocol for WSN. This protocol operates in two phases namely as establishment of session key and data dissemination with hop-by-hop authentication. The Limitations of their scheme is energy optimization.

K. Singh et.al [2] have proposed a Reliable Energy-efficient Data Dissemination (REDD) scheme for WSN. In their scheme the reliable data delivery strategy is used when a forwarding node fails. In this strategy, sink constructs a grid when no valid grid is present in the sensor field. M.Vigneshkumar et.al[4] have proposed a secure data transmission protocols are with ID-based settings, they have employed ID information and digital signature for verification. The advantage of their scheme is their security. The limitations are there existing computation and communication overhead.

K.Shanmugam et.al[5] have proposed a secure data transmission for cluster-based WSNs (CWSNs),in their scheme the clusters are formed dynamically and periodically. The limitations are the attack caused by a few compromised nodes can inject arbitrary amount of error in the base station estimate of the aggregate.

Sruthi K et.al [7] have proposed a secure and distributed data dissemination protocol that can be used for the secure and efficient dissemination of data in wireless sensor networks. Classical protocols like Drip, Dip and DHV have limitations like that they are not secured. The malicious users can disseminate malicious code to the network with these protocols.

AneesaFatima et.al [9] have proposed a major security vulnerabilities in data discovery and dissemination in WSNs. They have analyzed the security of DiDrip [9].

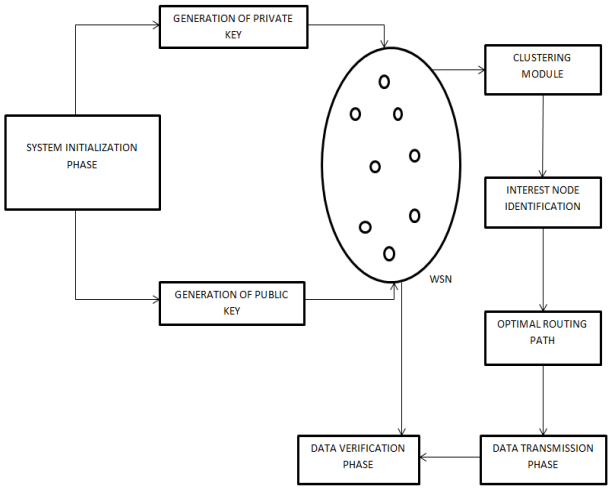
The limitation of DiDrip is open channel where messages can be easily intercepted. Savitri et.al [11] have proposed a secure and distributed protocol for data dissemination in wireless sensor networks. They have addressed the drawbacks of centralized approach of data dissemination. They provide data authentication by a secure hash function along with Merkle Hash Tree method for digital signature. The Data integrity is ensured by Elliptic Curve Cryptography. The limitations are there exists significant overhead and security should be enhanced further.

H. Jayasree et.al [14] have proposed a secure and distributed data discovery and dissemination protocol known as Di Drip. The DiDrip protocol is enhanced as EDiDrip to enhance the network life time in distributed wireless sensor network by using pre-failure rectification technique.

Anu M R et.al [15] have proposed a energy efficient security technique in WSNs. The advantage of the scheme is to protect the information that are transmitted by the sensor node, and improvement in throughput. The limitations are their security which is not considered in their design.

III. SYSTEM ARCHITECTURE

The proposed system architecture is shown in figure 1.



The proposed system consist of five phases namely System initialization phase, Cluster formation phase, Optimal routing phase, Data transmission phase, Packet verification phase. The detailed explanation of the proposed phases are explained as follows. In System initialization phase public and private key are generated. The deployed nodes forms a group of clusters in cluster formation phase. After the nodes are clustered the interested nodes are identified and optimal routing path is generated to provide energy efficient data dissemination. In data transmission phase the data is send to interest of nodes and in data verification phase ,the data validation is done by sensor nodes which are requested if the validation is successful ,the nodes install the data else the data packets are rejected.

IV. PROPOSED SYSTEMS

4.1 System Initialization Phase:

In system initialization phase, first the nodes are deployed in a random manner under 2D plain. The public and private key are generated and preloaded in each node of the network. The main role of system initialization phase is generation of public key and private key by using Elliptic curve cryptography algorithm [11]. The algorithm for generation of private key and public key is given as follows.

ALGORITHM 1:

Step 1: Choose a random integer X from the range [1……n-1], where n$\in$ z*P, where z*n^2 is the set of prime numbers.

Step 2: Compute the point $P1=X^{G1}$, where G$\in$z*q, where q is a set of prime numbers.

Step 3: Compute $r1=X1^{P1}$Modq

Step 4: Choose S1, S2 $\in$ E, where E is the elliptical curve point multiplication function.

Step 5: PuK = P1.S1 Mod q (1)

Step 6: PrK = r1.S2 Mod q (2)

The equation (1) and equation (2) gives the public key and private key.

4.2 Cluster formation phase:

In cluster formation phase, base station forms a cluster by considering hop distance and energy. The nodes which have high energy and less distance from the base station is considered as cluster head (CH). Only the CH are given privileges to communicate with base station. The steps for cluster formation is given algorithm 2

ALGORITHM 2: Cluster Formation

Step 1: Let X={x1,x2, ….xn} be the set of nodes deployed in the sensing domain.

Step 2: Initialize clustering level = {N to N+1}

Step 3: Initialize dist() and store in array namely array_dist[100].

Step 4: for all the nodes present in the network

Compute dist(BS,DN)

if{ Dist(Bs,X1)<=threshold

then

Increment cluster_level = 1}

End if

Step 5: Compute (dist(BS,DN))

if (dist(BS,N)>=cluster level

then

Increment cluster_level =2

End if

Step 6: Repeat steps 5-6 for all the nodes

Step 7: Compute (dist(BS,N))

if (dist(BS,N)>=cluster level 2

then

Increment cluster_level =3

End if

Step 8: Compute (dist(BS,N))

If (dist(BS,N)>=cluster level 2

then

Increment cluster_level=4

End if

Step 9: Check(If N == Empty)

then

Terminate the process

Else

Repeat steps(5-8)

End

4.3 Optimal routing path:

Optimal route will be selected based on the data transmitted. Optimal routing is the shortest and preferred route over which to transfer data from the source node to the destination node. The algorithm for optimal routing is explained in algorithm 3

ALGORITHM 3:

Step 1: Initialize Routing_Process () function and Initialize Route_array () function.
Step 2: BS →Identify(SN,DN) for all source present in the network.
Step 3: BS →(RR,CH) , CH →Respond(RR) for all the nodes present in network.
Step 4: BS calculates distance[SN,DN]
BS →calculates dist[SN,DN]
BS →RE[SN,DN]
If(dist = = high && R.E = = high)
then
choose path as very high priority_path;
If(dist = = high && R.E = = low)
then
choose path as medium priority_path;
If(dist = = low && R.E = = high)
then
choose path as high priority_path;
If(dist = = low && R.E = =low)
then
choose path as low priority_path;
Step 5: Compute priority_route ={priority_path}
Step 6: Store priority_path →{ Route_array}
Step 7: Terminate the process

4.4 Data transmission phase:

After finding optimal routing path the data is transmitted to interest of nodes with the sender public key. The group of nodes which have been selected by interest node identification will be transmitted in this phase. The message format for data transmission phase is given as:

D_{PT} = h (DDP||PUK)

Where D_P is Dissemination packets
h is hash function
DDP is Data dissemination packets
PUK is public key

4.5 Data verification phase:

In data verification phase transmitted data is send to interest of nodes, and the data validation is done by sensor nodes with their private key. If the validation is successful , the nodes install the data else the data packets are rejected. The message format for data verification phase is given as:

D_{VT} = h (DDP||PRK)

Where D_V is Data verification
h is hash function
DDP is Data dissemination packets
PRK is private key

V. EXPERIMENTAL SETUP AND SIMULATION PARAMETERS

The feasibility of proposed protocol is implemented by using NS2 simulator. Table 1 gives simulation parameters of the proposed protocol.

Table 1. Simulation Parameters

Network simulator	NS2
Simulation area	100m
Density of nodes	600 – 1000
Transmission range	30-35m
Node initial energy	10J
Simulation duration	70 minutes
No of trails	70
Packet size	20bytes

VI. RESULTS AND DISCUSSIONS

The performance evaluation of the proposed protocol is carried in term of node energy consumption, node life time and packet delivery ratio.

A. Node Energy Consumption

Figure 1 gives the Node Energy Consumption of proposed system then it compares with other existing protocols from the graph. It is clear that, the proposed protocol identifies the nodes which are required for data dissemination and transmits the dissemination packets through Intelligent routing. By doing so, the proposed protocol is able to reduce the redundant transmission and retransmission of both data packets and control packets. Hence the proposed system has better node life time compared with other existing protocols.

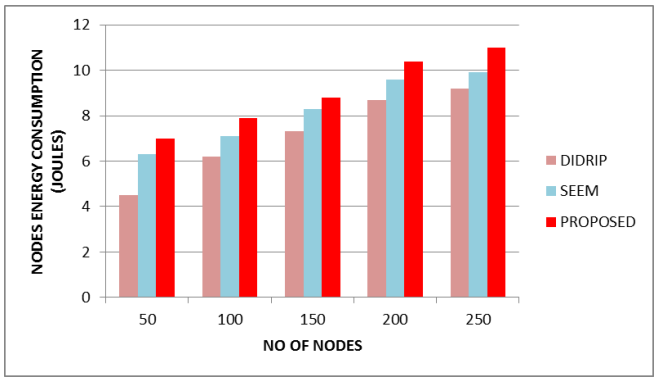


Figure 1 Node Energy consumption

B. Node Life Time

Figure 2 gives the nodes life time of proposed system then it compares with the other existing protocol. This protocol identifies the malicious nodes and removes it from the routing path. Moreover the proposed protocol reduces the packet drop by the malicious nodes. By doing so, the proposed protocol has better node life time compared with the existing protocol.

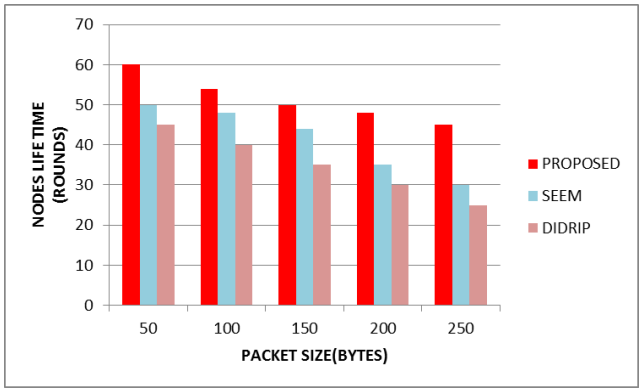


Figure 2 Node life time

C. Packet delivery ratio

Figure 3 gives the packet delivery ratio of proposed system then it compares with the other existing protocol. The packet delivery ratio of proposed protocol is better because proposed protocol provides security against malicious nodes and prevents them dropping of packets. Hence the proposed protocol has better packet delivery ratio compared with other existing protocols.

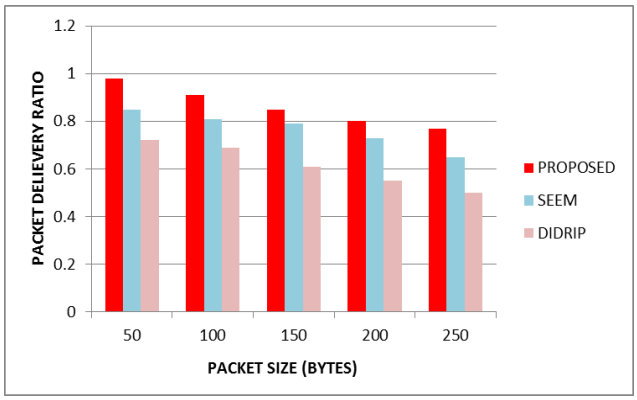


Figure 3 Packet delivery ratio

VII. CONCLUSION AND FUTURE WORK

In this paper, a novel secured data dissemination protocol has been proposed to provide security during data dissemination. The proposed protocol is implemented using NS2 simulator. The simulation results justifies that the proposed protocol has better node life time and optimized node energy consumption and better packet delivery ratio. Future work of the proposed system can be done by enhancing this protocol for mobile nodes.

REFERENCES

1. kumar, n., kumar, m. And r.b, p. (2019). A secure and energy efficient data dissemination protocol for wireless sensor networks. International journal of network security, 15(6), pp.pp.490-500.
2. k, s. And t.p, s. (2013). Redd: reliable energy-efficient data dissemination in wireless sensor networks with multiple mobile sinks. International journal of electronics and communication engineering, 7(6).
3. xl, z. And m, w. (2019). A survey on data dissemination in wireless sensor network. Journal of computer science and technology, 29(3), pp.470-486.
4. m, v. And s.k, m. (2015). A survey on secure and efficient data transmission for cluster-based wireless sensornetworks(cwsn). International journal of science and research (ijsr), 4(12), pp.1152-1154.
5. k, s., b, v., raja, a., r.a, p. And shiny, s. (2015). Secure and efficient data transmission in wireless sensor network using set protocols. Ijedr, pp.2321-9939.
6. k, r. And e, b. (2015). Efficient energy utilization path algorithm in wireless sensor networks. International journal on cybernetics & informatics, 4(2), pp.53-63.
7. k, s. And panicker, b. (2016). Sec-didrip: a distributed data dissemination protocol with enhanced security. International journal of advanced research in computer and communication engineering, 5(1).
8. kaur thind, n. And kumar, e. (2016). Efficient transmission in wireless sensor network using abs technique. Ijcsmc, 5(7), pp.pg.36 – 43.
9. fatima, a. And nase, g. (2016). An efficient and secure data dissemination protocol for wireless sensor network. International journal of combined research & development, 5(6).
10. n.b, k., priya, p., komal, t. And ashwini, g. (2016). Secure data discovery and data dissemination in wsn using didrip protocol. Ijariie, 2(2).
11. sridhar, s. (2016). Distributed and secure didrip protocol for data discovery and dissemination in wsns. International journal of innovative research in science, engineering and technology, 5(4).
12. b, g. (2016). Survey on secure and distributed data discovery and dissemination in wsn. International journal of engineering research and general science, 4(2), pp.2091-2730.
13. gupta, n., tayal, s., gupta, p., goyal, d. And goyal, m. (2017). Evaluation of data dissemination and discovery of routing protocol in mobile wireless sensor network. Issn, 10(3), pp.pp. 505-509.
14. h, j. And n, s. (2018). Secure data dissemination in wireless sensor networks using enhanced didrip. Indian j.sci.res., 17(2), pp.52-525.
15. m r, a. And l, s. (2019). Energy efficient secure communication in wireless sensor networks: a survey. International research journal of engineering and technology (irjet), 06(04).
16. Santhosh Kumar SVN, M. Selvi, A Gayathri, Ruby D, A Kannan, “Energy Efficient Rule based intelligent routing using Fitness Functions in Wireless Sensor Networks”, international Journal of Innovative Technology and Exploring Engineering (IJITEE), Vol 8 (12),PP.5414-5420
17. Rakesh Rajendran, SVN Santhosh Kumar, Yogesh Palanichamy, Kannan Arputharaj, “Detection of DoS attacks in cloud networks using intelligent rule based classification system”, 22 (1),pp 423-434, 2019.
18. M Selvi, K Thangaramya, Ganapathy Sannasi, K Kulothungan, H Khannah Nehemiah, A. Kannan, “An Energy Aware Trust Based Secure Routing Algorithm for Effective Communication in Wireless Sensor Networks”, pp 1-16.
19. K Thangaramya, K Kulothungan, R Logambigai, M Selvi, Sannasi Ganapathy, A Kannan, “Energy aware cluster and neuro-fuzzy based routing algorithm for wireless sensor networks in IoT”, vol 151, pp 211-223.

AUTHORS PROFILE

S. V. N. Santhosh Kumar is an Assistant Professor in VIT-Vellore Campus, India. He works in the areas of security and data dissemination in wireless sensor networks. His areas of interests include Wireless Sensor Networks, Internet of Things, Mobile Computing. He received his B.E. degree in Computer Science and Engineering and M.E. degree in Software Engineering and Ph.D. from Anna University, Chennai, India in the years 2011, 2013 and 2017

U. Nandhani is currently perusing Master of Software Engineering in School of Information Science and Technology, VIT University, Vellore, India. Her areas of interest are Wireless Sensor Networks and Data mining