iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 2 **Issue:** VII **Month of publication:** July 2014

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

ISSN: 2321-9653

INTERNATIONAL JOURNAL FOR RESEARCH IN APPLIED SCIENCE AND ENGINEERING TECHNOLOGY (IJRASET)

Light Weight Cryptography Based Secure Routing in Wsn

Monika Verma[#1], Madhu Bhatia[#2],Deepak Goyal[#3]

1M.Tech. Student, Deptt. of CSE, VCE Rohtak, Haryana(India)
2Asstt. Prof., Deptt. of CSE, VCE Rohtak, Haryana (India)
3 Asso. Prof., Deptt. of CSE, VCE Rohtak, Haryana (India)

Abstract- Wireless networks are usually more vulnerable to various security threats as the unguided transmission medium is more susceptible to security attacks than those of the guided transmission medium. The broadcast nature of the wireless communication is a simple candidate for eavesdropping. In most of the cases various security issues and threats related to those we consider for wireless ad hoc networks are also applicable for wireless sensor networks. The data encryption standard is highly secure algorithm. The DES is very complex so increases the delay that reduces the packet delivery ratio in network. The light weight secure algorithm may decrease the end 2 end delay to improve the performance. The light weight algorithm must be highly secured. The proposed work introduces the light weight cryptography algorithm that improves the performance of the network without compromising the security in the network. The authentication check by using the proposed algorithm is done at each intermediate node. If the security check fails then the node is discard else the data is forwarded to next node. The performance comparison is done using the PDR and e2edelay. The results show that the proposed algorithm is better than the existing algorithm as the PDR is improved and the e2edelay is decreased.

Keywords- WSN, DES, light weight Cryptography.

I. INTRODUCTION

Wireless sensor network (WSNs) consists of distributed autonomous sensors that communicate with each other in a wireless environment and are monitored by a base station. Sensor nodes gather information from environments and communicate[1] with the base station which acts as a gateway to connect other networks.[2] WSNs are used in military surveillance, real-time traffic monitoring, forest fire detection, agriculture and many other areas. Multipath routing is a routing technique, which selects multiple paths to deliver data from source to destination. Thus, multipath routing plays an important role in WSNs .

The data encryption standard is highly secure algorithm. The DES is very complex so increases the delay that reduces the packet delivery ratio in network. The light weight secure algorithm may decrease the end 2 end delay to improve the performance. The light weight algorithm must be highly secured[4].

Data Encryption Standard (DES) is one of the encryption techniques used for the block cipher. It takes 64 bits data block as input with 56 bit key (after randomly generated from 64 bits). DES is comprised of three stages. Firstly, an initial permutation is done on the 64 bits input block which generates a permuted input to work with further. The second stage deals with the 16 rounds of iteration of same function with randomly generated keys at each round and a pre-output is generated [3]. The third stage consists of an inverse initial permutation that gives us our desired cipher block. And in The decryption technique in the DES is the same as encryption one with the only the difference that the application of the sub keys are reversed[5]. Authentication is ensuring that sensor nodes, cluster

heads and base stations are authenticated before granting a limited resource or revealing information. Authentication ensures a receiver that data, mobile code or control data such as route updates, location information and key management messages originates from the correct source [6].
Authentication Procedures: Different authentication procedures are as follows:

A. *One-way authentication*

Only a single message is sent from sender node to the receiver node, this message will be able to establish i: the identity of sender and that the message was generated by sender, ii: the message is intended to the receiver and iii: the message is not modified during transit.

B. *Two-way / mutual authentication*

Mutual authentication, also called two-way authentication, is a process in which both entities in a communication link authenticate each other. In sensor network environments, mutual authentication not only refers to authentication between the normal nodes and the base station, it can also refer to two counterparts that are assured of each other's identity.

C. *Three-way authentication*

This is an authentication process when the clocks of the nodes cannot be synchronized. A third message from the sender to the receiver is sent.

D. *Implicit authentication*

Implicit authentication is not performed as an independent process. Instead, it is the byproduct of other processes, such as key establishment. This authentication paradigm in wireless sensor networks can reduce operating complexity and minimizes power consumption.

II. PROPOSED WORK

The proposed work introduces the light weight cryptography algorithm that improves the performance of the network without compromising the security in the network. The authentication check by using the proposed algorithm is done at each intermediate node. If the security check fails then the node is discard else the data is forwarded to next node. The light weight cryptographic algorithm is given below:

1. Encryption Algorithm

1. Input Key
2. Input plain Text i.e. data
3. L=1
4. For i=1:length(data)
5. Newkey(i)=key(L)
6. Increment in L
7. If L>length(key)
8. L=L-length(key)
9. End if
10. End for
11. For i=1:length(data)
12. If i%2!=0
13. Newdata(i)=data(i) xor newkey(length(data)-i)
14. Else
15. Newdata(i)=data(i) xnor newkey(length(data)-i)
16. End
17. End for
18. Resultdata=newdata

2. Decryption Algorithm

19. Input Key
20. Input Cipher Text i.e. data
21. L=1
22. For i=1:length(data)
23. Newkey(i)=key(L)
24. Increment in L
25. If L>length(key)
26. L=L-length(key)
27. End if
28. End for
29. For i=1:length(data)
30. If i%2!=0
31. Newdata(i)=data(i) xor newkey(length(data)-i)
32. Else
33. Newdata(i)=data(i) xor(not(newkey(length(data)-i))
34. End
35. End for
36. Originaldata=newdata

III. PARAMETER ANALYZED

Various parameters used for analysis are described below:

1. Packet Delivery Ratio (PDR): The ratio of the number of delivered data packet to the destination. This illustrates the level of delivered data to the destination.

∑ Number of packet receive / ∑ Number of packet send

2. End-to-end Delay: The average time taken by a packet to arrive in the destination. It also includes the delay caused by route discovery process and the queue in data packet transmission. Only the data packets that successfully delivered to destinations that counted.

∑ (arrive time – send time) / ∑ Number of connections

TABLE 1 TABLE 4.1: PARAMETER ANALYSIS OF EXISTING ALGORITHM

Run	PDR	E2E Delay	Total packet
1	0.9978	0.3510	926
2	0.9967	0.3521	604
3	0.9984	0.3481	1213
4	0.9983	0.3424	1195
5	0.9983	0.3427	1205
6	0.9983	0.3345	1178

TABLE 2 TABLE 4.2: PARAMETER ANALYSIS OF PROPOSED ALGORITHM.

Run	PDR	E2EDelay	Total packet
1	0.9992	0.0046	1183
2	0.9992	0.0068	1225
3	0.9992	0.0082	1212
4	0.9992	0.0056	1215
5	0.9991	0.0048	1163
6 data	0.0092	0.0080	1195

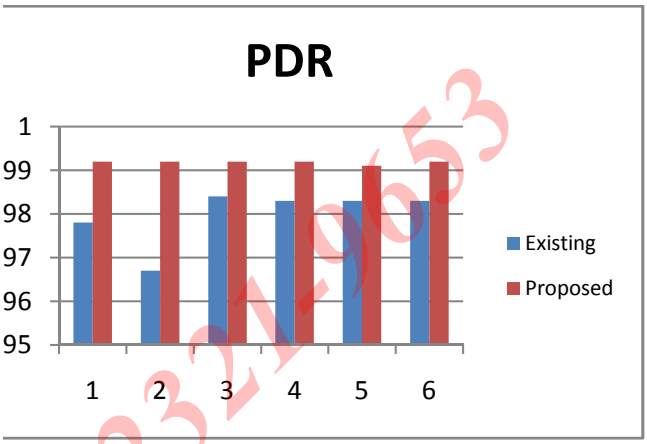


Figure 1: Comparison of PDR

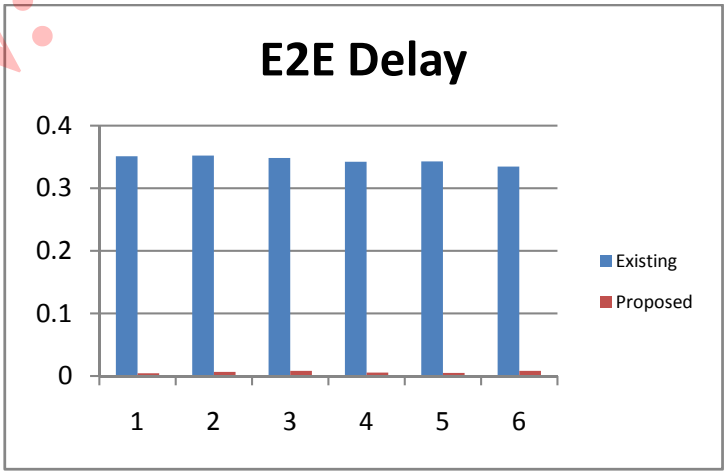


Figure 2: Comparison of E2E Delay

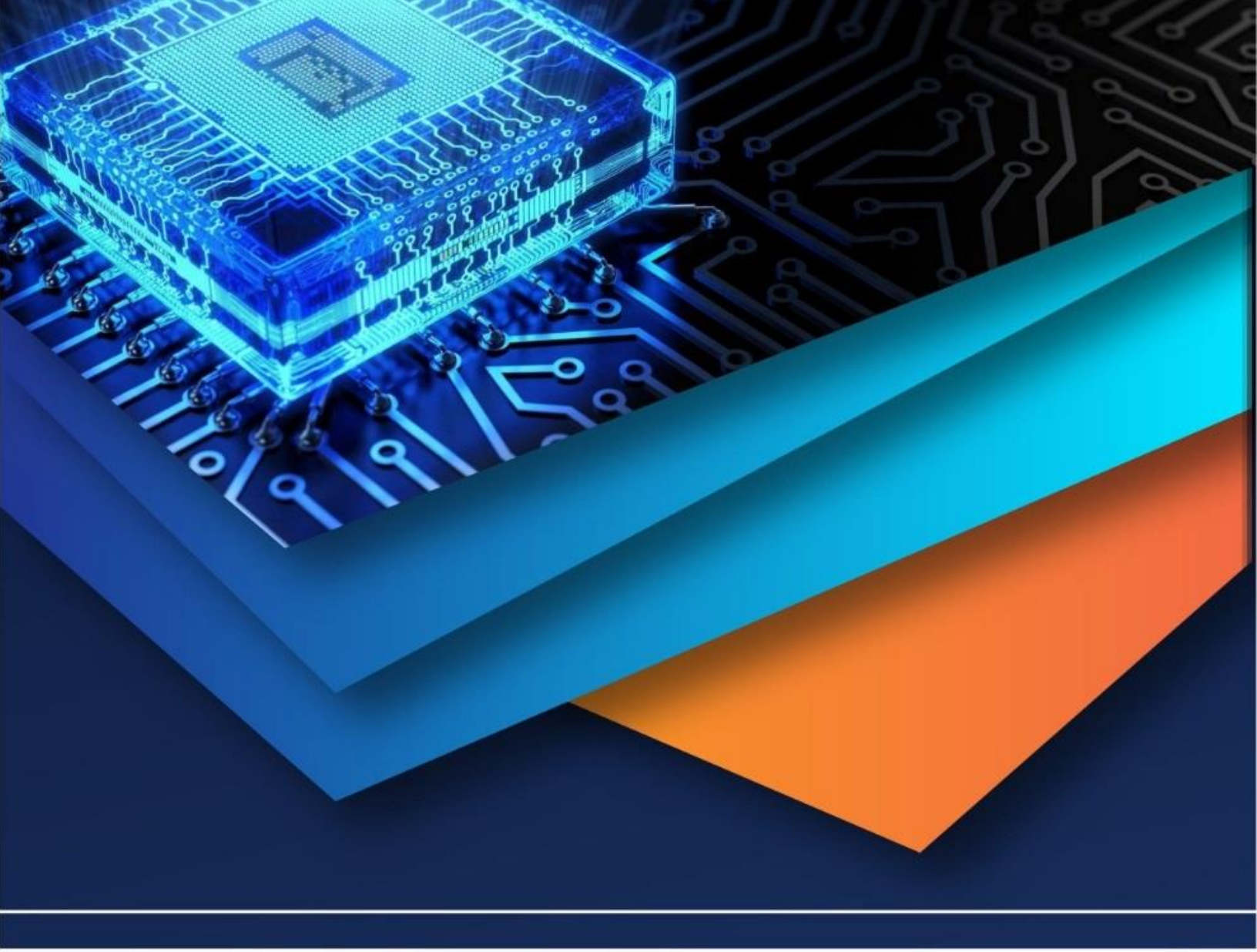
IV. CONCLUSION

The data encryption standard is highly secure algorithm. The DES is very complex so increases the delay that reduces the packet delivery ratio in network. The light weight secure algorithm may decrease the end 2 end delay to improve the performance. The light weight algorithm must be highly secured. The proposed work introduces the light weight cryptography algorithm that improves the performance of the network without compromising the security in the network. The

authentication check by using the proposed algorithm is done at each intermediate node. If the security check fails then the node is discard else the data is forwarded to next node. The performance comparison is done using the PDR and e2edelay. The results show that the proposed algorithm is better than the existing algorithm as the PDR is improved and the e2edelay is decreased.

REFERENCES

1. [1] Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. "A survey on sensor networks". Communications magazine, IEEE, 40(8), 102-114. (2002)..
2. [2]S.Suganya, P.Prabaharan ,L.Malathi, "A Survey on Multipath Routing Protocols for Reliable Data Transmission in Wireless Sensor Networks", Vol 2, Issue 11, November- 2013.
3. [3] Jayashree A, G. S. Biradar, V. D. Mytri, "Review of Multipath Routing Protocols in Wireless Multimedia Sensor Network –A Survey", Volume 3, Issue 9, September-2012.
4. [4] M. R. Pearlman, Z. J. Haas, P. Sholander, and S. S. Tabrizi, " On the impact of alternate path routing for load balancing in mobile ad hoc networks," in Proceedings of the 1st ACM international symposium on Mobile ad hoc networking & computing. Boston, Massachusetts: IEEE Press, 2000.
5. [5] Kumar, Gulshan, Mritunjay Rai, and Gang-Soo Lee. "Implementation of Cipher Block Chaining in Wireless Sensor Networks for Security Enhancement." International Journal of Security and Its Applications 6, no. 1 (2012).
6. [6] Shantala Patil , Dr Vijaya Kumar B P, Sonali Singha, Rashique Jamil, "A Survey on Authentication Techniques for Wireless Sensor Networks", Vol. 7 No.11 (2012).



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY