IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Issue-12, Dec 2019 E-ISSN: 2347-2693

Malicious Node Detection in Wireless Sensor Networks using Cryptographic Authentication and Certificate Revocation Mechanism

T. C. Swetha Priya[1*], A. Kanaka Durga[2]

[1,2]Dept. of Information Technology, Stanley College of Engineering and Technology for Women, Hyderabad, India

[*]*Corresponding Author: tcswethapriya@stanley.edu.in*

DOI: https://doi.org/10.26438/ijcse/v7i12.1620 | Available online at: www.ijcseonline.org

Accepted: 18/Dec/2019, Published: 31/Dec/2019

Abstract— Security is one of the major issues in the current scenario. Because of the wireless nature of the nodes present in Wireless Sensor Networks, there is a chance of the nodes getting easily affected to severe security attacks. One such attack is a Selective Forwarding Attack in which the malicious nodes gain access to the wireless network and interrupts the data communication, overwrites the data packets, drops the packets and degrades the wireless network performance. In this paper, an effective cryptographic protocol using Authentication technique is proposed. To separate the attacking nodes in participating in the future networking activities, a Certificate Revocation Method is also proposed. This paper guarantees security to the nodes and do not allow access to any of the affected nodes by using a more efficient Authentication method. It also improves the performance of a network. Through simulation, the correctness and efficiency of the scheme is verified.

Keywords— Authentication, Certificates, Cluster, malicious node, message digest, Revocation, Wireless Sensor Network.

I. INTRODUCTION

Because of the adhoc nature of Wireless Sensor Network and the inbuilt requirements of WSN there may be some challenges that are to be faced by such type of networks. So, security will become one of the major issues that influence the attackers to focus on severe attacks on the network. And because the nodes are distributed throughout the network there is a high chance of the corruption of data because of some malicious attacker nodes. A Wireless Sensor network is shown in Fig 1.

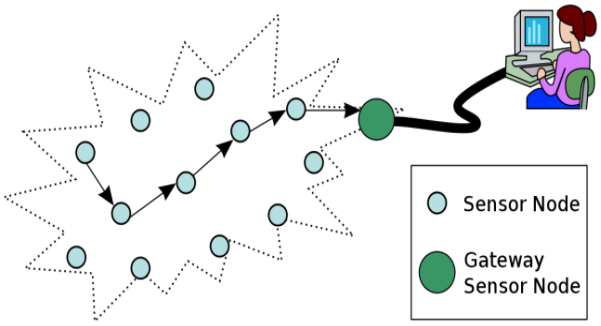

Figure 1. A Wireless Sensor Network

Wireless Sensor Network's may be prone to severe attacks. One such attack that is prominently known is Selective Forwarding attack. In this type of attack, during the transmission of data, the malicious nodes tries to gain access to network and tries to corrupt or interrupt the data. Sometimes these nodes try to drop some packets during transmission of data.

Hash algorithms have a significant role in cryptographic applications like securing passwords, authentication of nodes, data authentication, etc.,. This type of algorithms will take variable length data as input and generates fixed sized data called as Message Digest as output. Of these hash algorithms, one-way keyed hash functions are most commonly used. In this paper, MD5 algorithm is used for authentication of node identities.

So, in this paper an identity based light-weight Cryptographic Authentication based method is proposed to detect the malicious nodes. This method involves simple calculations.

Another important consideration is once a node is identified as malicious it should be avoided from all the activities that are being done on the network. So, whenever a node is identified malicious its identity has to be invalidated. This can be done by adding Certificate Revocation [5] Method as second layer of security.

II. RELATED WORK

Existing systems provides a hash based message digest method using less number of calculations and relatively less

© 2019, IJCSE All Rights Reserved

overhead. But they are not effective in terms of utilizing the message digest [1][6] in the authentication of nodes or authentication of messages.

These systems are able to separate malicious nodes using revocation of Certificates [4][5]][7] but they are unable to provide authentication for the nodes using one-way hash functions.

Some of the systems used fuzzy logic in revoking the certificates of the affected malicious nodes. But using this fuzzy logic for separating the nodes can be a bit costly. So this type of method is not preferable.

Some of the methods used voting mechanism [4] to choose clusters and then use certificate revocation method for invalidating these certificates. But this system do not provide additional layer of security. This also do not provide good throughput and efficiency.

So, some of these existing systems are facing many challenges such as lack of security, more overhead, packet drop, delay in the forwarding of packets, no data hiding and less throughput. So, there is a need for a more efficient scheme to overcome these problems.

III. PROPOSED SYSTEM

The proposed system is divided into 3 basic functions:
a) Authentication of Nodes
b) Securing the information using MD5 and
c) Revocation of malicious node certificates.

A. Authentication of Nodes

In this method, we pick some nodes randomly and mark these nodes as temporary server nodes. Every node is assigned an identity or ID which is unique. Each sender node will create a pair of keys [8] and transmit the information to temporary server node. This temporary server will authenticate [3] the sender nodes identity and then if the node is valid one then the information will be transmitted to the destination. If the nodes' authentication fails, then the sender node is marked as a attacker node.

1. Algorithm for Authentication of Nodes

1. Choose a node as Temporary server node for authenticating the rest of the nodes.
2. Each node must be identified with an identity that is unique.
3. Sender will create a pair of keys.
4. Then the sender will transmit information to the Chosen server.
5. This server will authenticate the sender's identity.
    a. If the sender node is a valid node, then
        i. Data will be forwarded to the destination node.
    b. Else
        i. Sender node is marked as malicious node.

B. Securing the information using MD5

Once the node is identified as a malicious node, the sender node's information will not be sent directly to the destination. Only the hash value of the message will be transmitted. So, the proposed method uses a Cryptographic hash function that is based on One-way Keyed hashing algorithm, MD5 to hide the original data from other nodes. This algorithm will take variable length data as input and generates fixed sized data of 128-bits called as Message Digest as output. One restriction for MD5 hashing algorithm is that no two messages should have the same message digest. And also there should not be same hash value for different messages.

The MD5 hash algorithm [1] [6] will generate a 32-bit hexadecimal hash value as shown in Fig 2. This algorithm first divides the variable length information into some part. Each part should be of 512-bits. If any part of the message could not form 512-bits then some extra bits are appended to that part to make it a multiple of 512. This appending uses a modulo exponentiation method.

```
Node(0) --> c4dfd145e649849eb4a66f83c052a8de
Node(1) --> a9913d1a1eaccaa08606200dc92faaac
Node(2) --> 31de96583d142dd056ee4aa8e414d2f7
Node(3) --> 251be14410ba28c9ab8390af4938f818
Node(4) --> 54b62bf67f4db2aa4b457af2f3aa074a
Node(5) --> cc651450d37686b8e50907e24e777408
Node(6) --> f109638ef552198f3ef39ec6ec63df90
Node(7) --> af5867e83e6ebd7a2882d65a7ef2967b
Node(8) --> c4dfd145e649849eb4a66f83c052a8de
Node(9) --> a9913d1a1eaccaa08606200dc92faaac
Node(10) --> 30c5361cec658aadf8c5d507b480abff
Node(11) --> 3ea0ab55ebe28186a7ab538539ff6d6b
Node(12) --> b9cc97ad5d0f54ad05b1f4a25ae592ef
Node(13) --> 29085b1915158d918c645218292aba02
Node(14) --> 01bcbb824aa1d6fd6b9bf6ca4306b6ec
Node(15) --> 63f02696eab950eda8d1b33b5ce9a150
Node(16) --> 18a5dbee810d0eb5efc52c8c9e0a835b
Node(17) --> bfe18b5a995da33fe91cb2c12d397da5
Node(18) --> 8a1187f64554bd178eb126760383b11d
Node(19) --> 47ca8d8618763bdcfb41d146f13a4d91
```

Figure 2. 32-bit hexadecimal hash value generation

C. Revocation of malicious node certificates

Once if the nodes are identified as malicious, the immediate action that is to be taken is to separate these attacker nodes from further interacting with the network and performing the network activities. So, there is a need for Revocation of certificates.

The network is partitioned into many separate clusters [2][10]. Then a voting mechanism [4] is employed for election of a Cluster Head node for each and every cluster. The Cluster Head nodes will have a database of all the

© 2019, IJCSE All Rights Reserved

certificates i.e., keys of all the nodes present in the cluster. The node that is found to be malicious will not be allowed to participate in any of the future network activities by revoking that particular nodes certificate or the keys. So, if a node's certificates are revoked [7] [9] then it cannot be able to communicate with any of the nodes in the future. In this way, the Selective Forwarding attack can be stopped to affect the network's performance.

IV. RESULTS AND DISCUSSION

In this scenario, a network comprising of 20 nodes is taken. Fig 3 shows the arrangement of nodes in the wireless network environment.

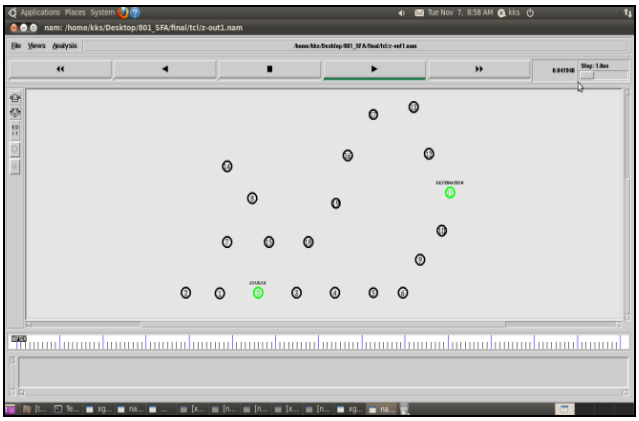

Figure 3. Arrangement of Nodes in the network

Fig 4 displays the malicious behavior of the nodes. In the simulation the malicious node is trying to reroute the nodes path.

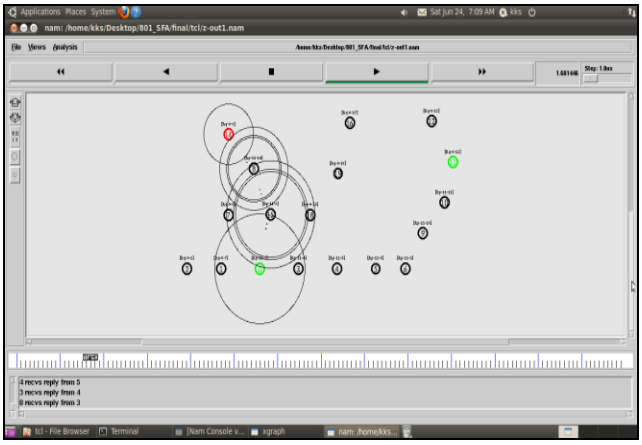

Figure 4. Malicious node Behavior

Here, the temporary servers will maintain two separate lists: Malicious nodes, Non-malicious nodes list. In simulation, the nodes that are identified as malicious are marked in red color as shown in Fig 4. Fig 5 shows how malicious nodes are separated from communication of information. Fig 6 shows transmission of data after recovery from malicious nodes. The malicious nodes are separated from the network and are not allowed to take part in any of the further communication of information over the network. Fig 7 shows the Selection of Cluster Heads in the clusters formed. These cluster heads keep track of keys and certificates of the malicious node and invalidates them.

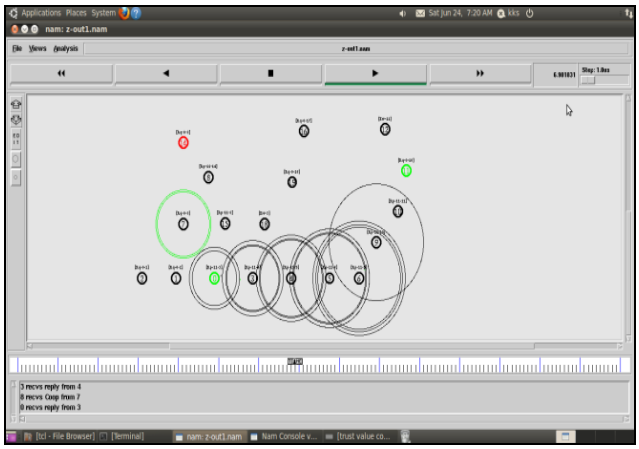

Figure 5. Identification of Malicious node

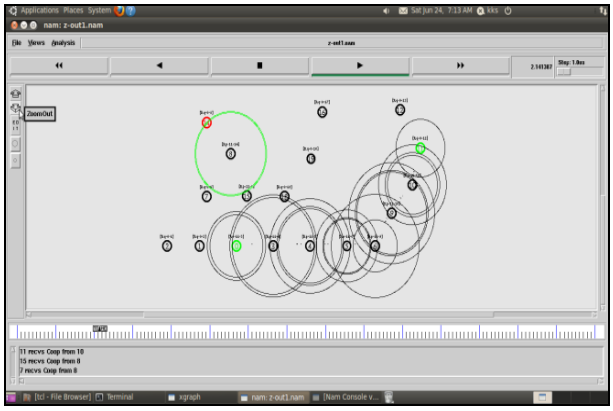

Figure 6. Transmission of data in the network

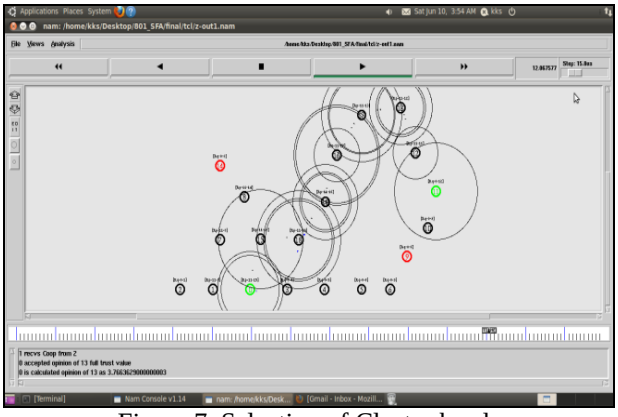

Figure 7. Selection of Cluster heads

© 2019, IJCSE All Rights Reserved

V. PERFORMANCE EVALUATION USING SIMULATION

As the proposed system is able to separate malicious nodes using Revocation of certificate mechanism, the throughput of the proposed system is more when compared to the existing system. Fig 8 shows Improvement of Throughput in proposed system when compared to existing system. As the malicious nodes are separated from the network, there will not be any packet loss. So this improves the packet delivery ratio of the networks. Fig 9 shows improvement in the packet delivery ratio of the network.

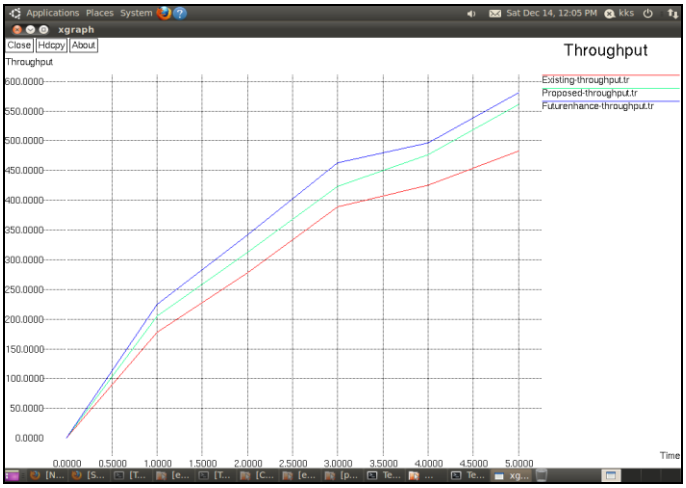

Figure 8. Graph showing Improvement of Throughput in proposed system

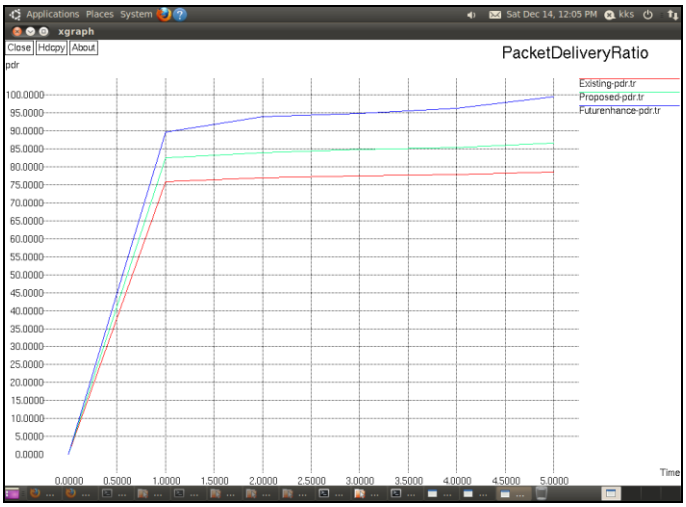

Figure 9. Graph showing Improvement of Packet Delivery Ratio in proposed system

Fig 10 and Fig 11 shows the reduction in the packet drop rate and the delay in proposed system.

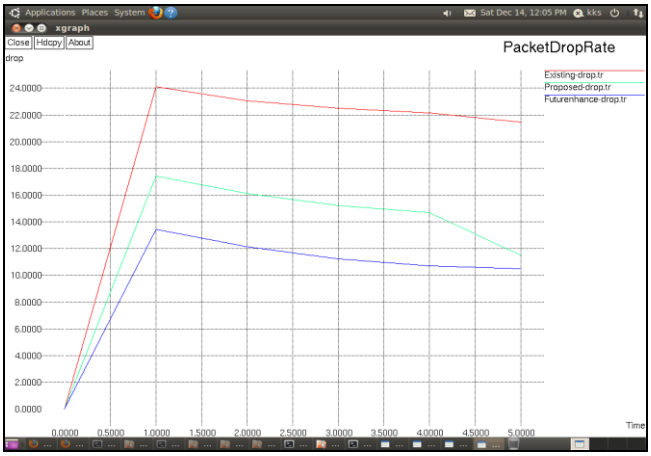

Figure 10. Graph showing reduction of packet drop rate in proposed system

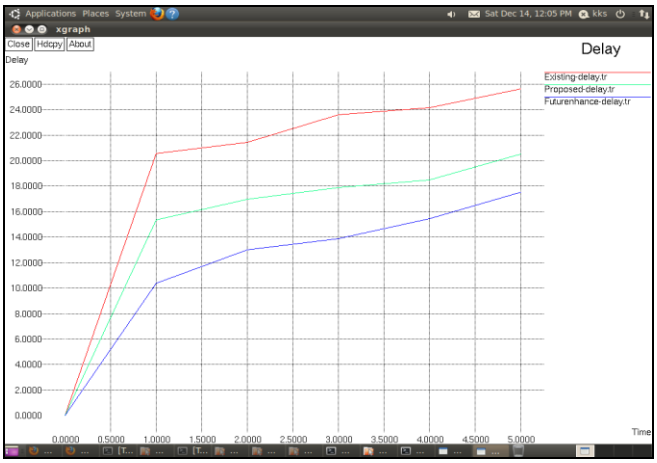

Figure 11. Graph showing reduction of delay in proposed system.

VI. CONCLUSION

In the proposed system, we provide security to the network by separating malicious nodes from the network. It first provides authentication to the nodes. Once the malicious nodes are identified, then an additional layer of security is provided by using the revocation method. This provides security to the nodes by not allowing them to perform any further activities on the network. This improves the network performance and also increases throughput. The data will be secured by using a one way hash function using MD5. This feature provides security to the information. But the proposed system do not focus on energy saving of the nodes.

VII. FUTURE SCOPE

In future, an efficient mechanism that is based on energy saving of the nodes will be added to the proposed system. This work can be further extended to include mobile nodes where the security will become more complicated.

© 2019, IJCSE All Rights Reserved

REFERENCES

[1] Aggarwal, S., Goyal Astt Professor, N., & Aggarwal Astt Professor MRCE, K. (2014). "A review of Comparative Study of MD5 and SHA Security Algorithm". International Journal of Computer Applications.

[2] Wei Liu, Student Member, IEEE, Hiroki Nishiyama, Member, IEEE, Nirwan Ansari, Fellow, IEEE, Jie Yang, and Nei Kato, Senior Member, IEEE "Cluster-Based Certificate Revocation with Vindication Capability for Mobile Ad Hoc Networks".

[3] Youtao Zhang, Jun Yang, Weijia Li, Linzhang Wang, Lingling Jin: "An authentication scheme for locating compromised sensor nodes in WSNs", Journal of Network and Computer Applications, vol.33, pp.50-62, 2010.

[4] Sungwook Kim, "Effective Certificate Revocation Scheme based on Weighted Voting Game Approach", IET Information Security, Vol. 10, No. 4, pp. 180-187, 2016.

[5] K. Park, H. Nishiyama, N. Ansari, And N. Kato, "Certificate Revocation To Cope With False Accusations In Mobile Ad Hoc Networks", In Proc. 2010 Ieee 71st Vehicular Technology Conference: Vtc2010-Spring, Taipei, Taiwan, May 16-19, 2010.

[6] Madhumita Panda, "Security in Wireless Sensor Networks using Cryptographic Techniques", American Journal of Engineering Research (AJER) 2014 Volume-03, Issue-01, pp-50-56.

[7] Priti Rathi, Parikshit Mahalle, "Certificate Revocation in Mobile Ad Hoc Networks," International Journal of Application or Innovation in Engineering & Management, Volume 2, Issue 1, January 2013.

[8] Khawla Naji Shnaikat and Ayman Ahmed AlQudah, "Key Management Techniques in Wireless Sensor Networks", International Journal of Network Security & Its Applications (IJNSA) Vol.6, No.6, November 2014.

[9] Claude Crêpeau and Carlton R. Davis," A Certificate Revocation Scheme for Wireless Ad Hoc Networks" School of Computer Science, McGill University, Montreal, QC, Canada H3A 2A7.

[10] E.K. Neena and C. Balakrishnan,"Cluster Based Certificate Revocation of Attacker's Nodes in MANET", International Journal of Computer Science and Engineering(IJCSE), Vol 2, Issue 1, January 2014

Authors Profile

Mrs. T.C. Swetha Priya is currently working as an Assistant Professor in Department of Information Technology at Stanley College of Engineering and Technology for Women, Hyderabad, India. Her Areas of Interest are Computer Networks, Information Security, Network Security, Data Structures. She has published 2 papers in International Journals. She has presented and published one paper in National Conference and another one in Springer Nature International conference. She has 3 years of teaching experience.

Dr.A.Kanaka Durga is currently the HOD of Department of Information Technology at Stanley College of Engineering and Technology for Women, Hyderabad, India. Her Areas of Interest are Data Mining, Information Retrieval Systems, Machine Learning, Semantic Web, Cloud Computing, Data Security, Cognitive Science, Big Data. She has over 22 years of teaching experience. She has published over 24 papers in National and International Journals and conferences.

© 2019, IJCSE All Rights Reserved