International Journal of Engineering & Technology, 7 (4.7) (2018) 152-156

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper



Identification and Avoidance of Malicious Nodes by using Certificate Revocation Method

H. Vamshi krishna[1]*, Gandharba Swain[2]

Department of Computer Science and Engineering, koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh, 5220502.
**Corresponding author E-mail:vamshi.janaki11@gmail.com*

Abstract

There are a large number of applications of ad-hoc networks (i) military, (ii) Disaster rescue, (iii) Medical etc. But the security of the data during transfer is a major concern. This paper proposes a technique for identifying and preventing the malicious nodes to be in a path from sender to receiver, known as certificate revocation method. Here certificate authority Scheme (CAS) is responsible for the issue of the certificates for these nodes. The CAS maintains two sets of lists – a warning list and a blocked list. The node is added to a warning list if any of the neighbor nodes raises a suspension about a node. Both the accuser and the accused are added to this list. The node is transferred to blocked list when the corruption in the node is confirmed. A node from the blocked list is never added to the network again. This process is termed as cluster-based certificate revocation scheme (CBCRS). The priority of this technique is not the detection of the corrupted node but the removal of the corrupted node from the network. Experimental results reveal that this protocol is free from vulnerabilities.

Keywords*: Certificate authority scheme (CAS); cluster-based certificate revocation scheme (CBCRS); fixed infrastructure; mobile Ad-hoc networks; malicious avoidance certificate revocation.*

1. Introduction

Ad-hoc networks are highly demanded network technology applications. The term ad-hoc means temporary. In ad-hoc networks nodes communicate with each other by single or multiple hops. Networking is made via cluster of nodes, these nodes helps in transferring the data without any means of authorization from the server. Thus these nodes are important for generating as well as managing the network [4]. An ad-hoc network does not use the infrastructure to communicate instead it use wireless network channel such as Bluetooth to communicate directly with each other. These types of networks are mainly used in disaster zones, military operation and also in required medical areas, where infrastructure no longer exists in using Wi-Fi or cellular networks. In Mobile Ad-hoc Network (MANET) [1] the nodes performs both router and host operations. There are several routing protocols such as proactive, reactive and hybrid protocols for routing purpose. Proactive stores the routing data of every node by means of destination sequenced distance vector (DSDV), optimized link state routing protocol (OLSR) and wireless routing protocol (WRP) algorithms. Whereas reactive implements on-demand routing protocols which means path is created when the source tends to send the data to destination by means of ad-hoc-on demand distance vector (AODV) [12], dynamic source routing (DSR) [3]. Hybrid routing protocols enhances both proactive and reactive protocols zone routing protocol (ZRP), temporary ordered routing protocol TORA and ordered one routing protocol OORP [5]. Ad-hoc networks face some security issues while transferring the data from source to destination. Several algorithms like DSR, AODV have been initiated to data transfer through secured path [6], [7]. In ad-hoc networking, the most significant part is to identify the route and transfer the data-packets from sender to receiver and also securing the data packets [10]. Most of the algorithms have solutions for implementing the route but failed to provide security. This leads unnatural behaviour of the nodes in network; these are known as malicious node. By this there may be chances of occurring disturbance in network during data transfer [8-11]. In this paper we discuss two things (i) identification of malicious nodes, and (ii) avoidance of malicious node using certificate revocation method (CRM). CRM implements two types of lists, (i) warning list, and (ii) blocked list. These lists helps in giving the warning if there are any chances of malicious node and the blocked list blocks the node and implements the other secure route to transfer the packets to destination.

2. Related work

It enhanced the previous version by improving the technique in identifying malicious nodes. This structure does not require any path to identify the route. This technique functions on a single way hash cryptographic module. In the networking process, the channel has to establish the communication between the nodes. Once the channel is online, the users can start sending the data.

Algorithm

Step1: select the cluster nodes.

Step 2: Generate data transfer for the private key.

Step 3: Send those keys to the respective nodes.

Copyright © 2018 Authors. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Step 4: Repeat step-2 for data transfer.

Step 5: Generate two tables for data implementation.

Step 6: A communication will be established by sender node to communicate with other node for providing time stamp.

Step 7: Nodes starts to communicate with each other and starts generating time stamps.

Step 8: Status message will be sent to each node which are in communication.

Step 9: Configure master server in two stages (i) verify sample time stamps that are collected and check for validity. If it finds to be invalid throw an error block, (ii) a relevant message is sent to all possible server nodes. Therefore Id-based corrupt node identification [2] technique only identifies the corrupted node but does not provide any prevention.

2. Proposed Work

The network requires three stages, (i) prevention of the node from getting corrected by issuing proper certification, (ii) Detection: If a node gets corrupted, immediately detect the malfunction and (iii) Revocation: Cease the permission for the node which is corrupted. It mainly functions under the following modules represented in fig.1 (i) Network module, (ii) Node analyzation module, (iii) Certificate Authority Scheme module, (iv) Routing level, (v) Verification Controller. The detailed explanation of each block is described below.

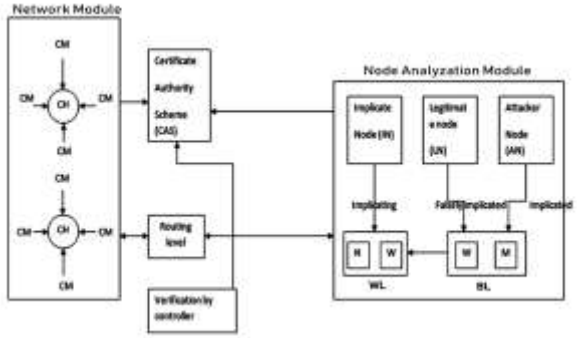


Fig. 1: Proposed framework

The network module consists of Cluster Heads (CH) and Cluster Members (CM). The certificate authority Scheme (CAS) is responsible for the issue of the certificates for the nodes. The CAS maintains two sets of lists – a warning list (WL) and a blocked list (BL). The node / CM is added to a warning list if any of the neighbor raises a suspension about a node. Both the accuser (N) and the accused (W) are added to this list. The node is transferred to blocked list when the corruption in the node is confirmed. The nodes in the blocked list never added to the network again. This process is termed as cluster-based certificate revocation scheme (CBCRS). The scope of the operation of the CAS is depicted below with the help of Fig2. The network consists of several nodes M, N, O, P and Q. The CAS block monitors the nodes in regular basis. In this scenario, M is the corrupted node and the other nodes N, O, P and Q are the target nodes, when these nodes detect that the node M is trying to attack them, a packet is sent to CAS with the required information. The CAS identifies the nodes and classifies them into accused and accuser. The CAS then tries to identify whether the node M is being targeted or is it genuinely corrupting the network. Later if it is true, the node is sent to blocked list.

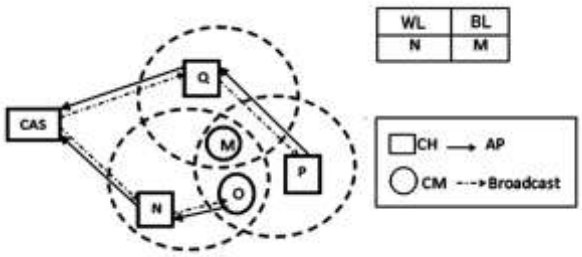


Fig.2: Certificate revocation process of a node in network

Algorithm: $ClusterHeadSelection$ **– CHS**

Input

Deployment Area WSN = $s \times s$,

- Set of sensor nodes $S = \{s_1, s_2, s_3, \dots, s_n\}$ s_i represents (x_i, y_i) the coordinate of i^{th} Sensor
- Transmission range T_r

Output
- CH–set of cluster heads

Begin

Step-1: CH selection is made.

Step-2: Calculate the distance between the nodes as $\sqrt{(X_2 - X_1)^2 + (Y_2 - Y_1)^2}$.

Step-3: The transmission range can be calculated as $T_{rp} = \pi \times d^2$.

Step-4: Calculate node degree $K_i^{tot} = K_i^{in} + K_i^{out}$.

Step-5: Calculate node mobility.

Step-6: Select CHs.

Step-7: CHs broadcasts membership message

Step-8: Set counter variable to 0.

Step-9: Receive a reply from a node and increment counter as counter = counter + 1.

Step-10: Node is added as member of the corresponding cluster

Step-11: CH nodes assigns certificate to its member nodes

Step-12: Sender node sends the message M_{ij} where i represent the sender node, j represents the receiver node, ID represents unique identity of node, n represents number of nodes, s represents trusted node, X represents hash value of node id.

$$M_{ij} =< ID_{ni}, ID_{nj}, T_{sij}, X >$$

Step-13: Initiates the communication.

Step-14: Generates message with timestamp T_s
Send the message to master server MS

MS generates the receiving timestamp T_r

Verify the timestamps of both sender and receiver. If Timestamp difference is small, mark the node as authorized node otherwise reject and mark as malicious. An accusation packet against malicious node is sent to CH it revokes the node as certified. The main priority of this scheme is not the detecting the attack but to removal of the corrupted node from the network.

3. Results and Discussion

The proposed system is simulated in the Network Simulator Software. In the implementation of the process, it is verified theoretically and conceptually and then performance of the system is discussed in terms of delay and through put.
In the simulation, the nodes participate in a hop by hop communication process. The distance between the nodes is assigned randomly and the nodes move based on as defined trajectory. Individual nodes communicate, and the data is exchanged in the form of packets.

Table 1: Network scale configurations

Node number	Field size (maxim)	No. of high level nodes	No. of connections
2	200x100	1	2
4	350x250	2	4
8	600x500	4	8
12	1000x500	8	10
16	1200x1200	10	12
20	1500x1500	14	16

Fig. 3 depicts the simulation pattern of the network. The total 20 of nodes are depicted in the image. The nodes are all assembled by the clustering process. In the process of communication each node is assigned a weight. This weight is calculated based on the following parameters, (i) Transmission range, (ii) Degree of node, (iii) Mobility factor. The node with the largest weight is claimed to be the Cluster head.



Fig. 3: The network topology

As mentioned in the previous diagram, the malicious nodes are identified by the certificate nodes and are revoked. The simulation process depicted in Fig. 4 shows the nodes and the certificate revocation process. The nodes 6, 10, 11, 15, 17 and 19, which are encircled twice, are treated to be in the blocked list and never given access again.

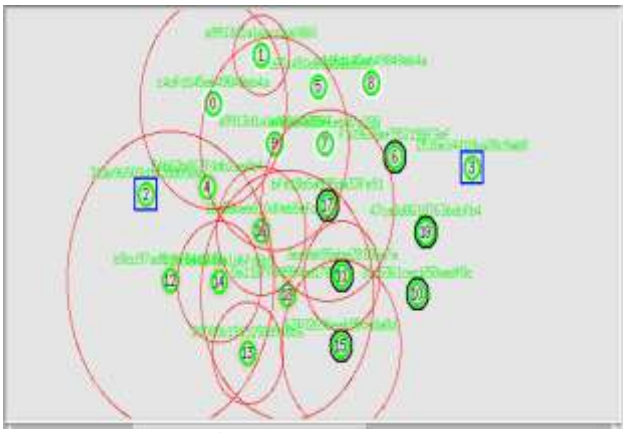


Fig. 4:, Certificate revocation process in network

The Fig.5 depicts a condition where a node is falsely identified as corrupted. This node is free to join the network and gains the right to communicate.



Fig. 5: False accusation formed by malicious node

Once the network is secure, the data communication process is initiated successfully and data is exchanged between the nodes. This process is depicted in Fig.6.

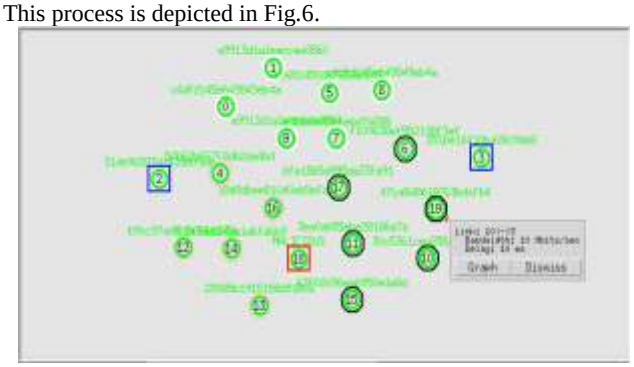


Fig. 6: Data communication by secure routing

Routing table and server key generation data depicted in the following Fig.7, Fig.8 measures,
(i) Hops, (ii) Next hop, (iii) Sequence numbers, (iv) Destination, (v) Flag points, (vi) Current time interval.

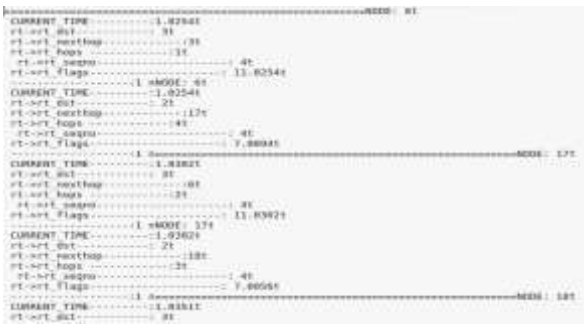


Fig.7: Routing table in network based on routing process

```
Node(0) --> c4dfd145e649849eb4a66f83c052a8de
Node(1) --> a9913d1a1eaccaa08606200dc92faaac
Node(2) --> 31de96583d142dd056ee4aa8e414d2f7
Node(3) --> 251bc14410ba28c9ab8390af4938f818
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) --> 10a5dbee810d0eb5efc52c8c9e0a835b
Node(17) --> bfe18b5a995da33fe91cb2c12d397da5
Node(18) --> 8a1187f64554bd178eb126760383b11d
Node(19) --> 47ca8d8618763bdcfb41d146f13a4d91
```

Fig. 8: Server data revoked keys

The four parameters which are used to present the efficiency of the proposed method are, (i) Packet propagation delay, (ii) Packet drop rate, (iii) Packet delivery ratio, (iv) Packet throughput.

Fig.9 through Fig.12 represents the comparison among (i) proposed CBCRS method (indicated by green), (ii) id- authentication method (indicated by red color) [2], N- AODV (indicated by blue color) [12].

Fig.9 compares the routing delay in network where AODV has high delay ratio and CBCRS has lowest delay ratio.

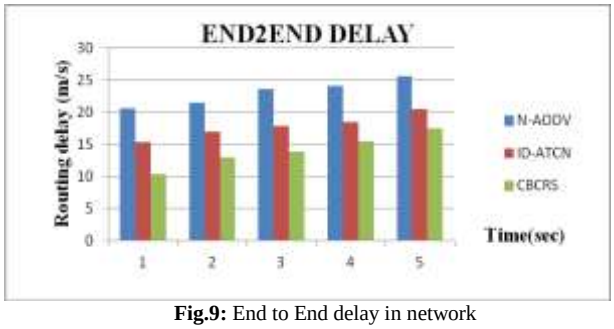


Fig.9: End to End delay in network

Fig 10 shows that, before data delivering check the route request (RREQ) and route reply (RREP) of nodes, the network throughput remains as high as the ID authentication method and N-AODV protocol while the network scale grows.

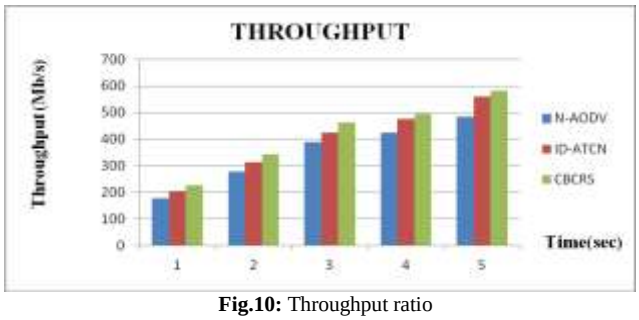


Fig.10: Throughput ratio

Fig.11 shows individual node data levels based on network routing process and routing levels.

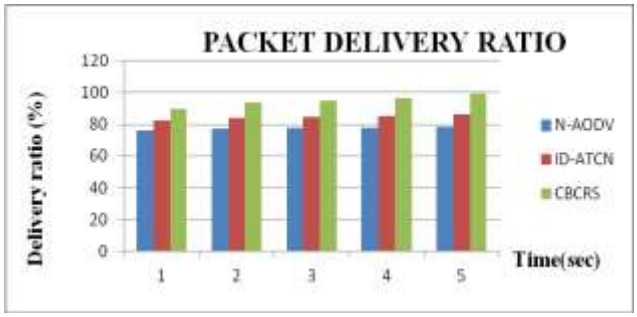


Fig.11: Packet delivery ratio

Fig. 12 shows, individual nodes drop ratio of the data based on effect from malicious nodes without knowing the behavior.

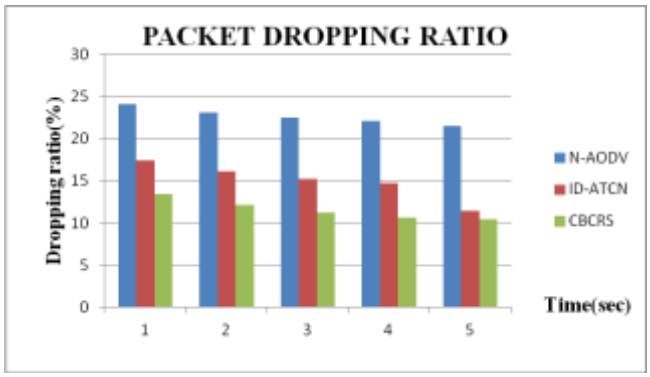


Fig. 12: Packet dropping ratio

Therefore, from above Performance of the CRM is immense when compared to other method.

4. Conclusion

This paper proposes a new algorithm for malicious node detection and prevention in ad-hoc networks for secure transfer of data. The proposed cluster based malicious avoidance certificate revocation scheme ensures secure network communication services for mobile ad-hoc networks. This CR method monitors the nodes regularly when these nodes are detected as malicious It identifies them as accused and then it makes the node as blocked list, thus gives the ability of distinguishing the erroneously accused node in the system and denies the authentication of that node to address the issue of false allegation. The performance of the proposed algorithm is investigated in terms of delay and thought put. It means nodes participate in a hop by hop communication process. From that malicious nodes are identified and certificates of these nodes are revoked. Hence, overall efficiency including performance evaluation claims that the protocol should be implemented in real life scenario. In comparison with existing schemes, a cluster based malicious avoidance revocation method is efficient. In the future, we will try to develop more efficient and increase of malicious nodes detection technique which is applicable for both wired and wireless networks.

References

[1] M. Rath, B.K. Pattanayak, B. Pati, "Energy efficient MANET protocol using cross layer design for military applications", vol.66, no.2 , pp.146-150, 2016.

[2] M.A. Abdelshafy, P.J.B. King, "Dynamic Source Routing under Attacks", 7th International Workshop on Reliable Networks Design and Modeling (RNDM), 2015, DOI: 10.1109/RNDM.2015.7325226.

[3] S.R. Das, C.E. Perkins and E.M. Royer, "Performance comparison of two on-demand routing protocols for ad hoc networks" , vol.8, no.1, pp.16-28, 2000.

[4] M. Manjunath, D. H. Manjaiah, "Spatial DSDV (S-DSDV) routing algorithm for mobile ad hoc network", 2014 International Conference on Contemporary Computing and Informatics (IC3I), DOI: 10.1109/IC3I.2014.7019587.

[5] J. Biswas, S.K. Nandy, "Efficient Key Management and Distribution for MANET", 2006 IEEE International Conference on Communications, DOI: 10.1109/ICC.2006.255106.

[6] H. Yang, H. Luo, F. Ye, S. Lu, L. Zhang, "Security in Mobile Ad Hoc Networks: Challenges and Solutions", vol.11, no.1, pp. 38-47, 2004.

[7] G.V.S Raju, R. Akbani, "Authentication in wireless networks", 2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07), DOI: 10.1109/HICSS.2007.93.

[8] Mamatha, G. Sharma, "A new secured approach for manets against network layer attacks", In, Integrated Intelligent Computing (ICIIC), 2010 First International Conference, DOI: 10.1109/ICIIC.2010.14.

[9] J.M. Chang, P.C. Tsou, H.C. Chao, Chen, J.L. chen,“ Cbds: a cooperative bait detection scheme to prevent malicious node for manet based on hybrid defense architecture”, 2011 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronics Systems Technology (Wireless VITAE), DOI: 10.1109/WIRELESSVITAE.2011.5940839.

[10] E. Nii, T. kitanouma, N. Adachi, , Y. Takizawa, “Cooperative detection for falsification and isolation of malicious nodes for wireless sensor networks in open environment”, 2017, DOI: 10.1109/APMC.2017.8251496.

[11] C. Perkins, E.B. Royer, and S. Das, “Ad hoc On-Demand Distance Vector (AODV) Routing,” Internet RFCs, vol. 285. pp. 1–38, 2003.