International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 - 5161

Available at http://inpressco.com/category/ijcet

Research Article

Threshold Based Clone Avoidance in AODV for Wireless Sensor Network

Sharanjit Kaur[Á*] and Mansi Gupta[Á]

[Á]Department of Computer Science and Engineering, Punjab Institute of Technology Kapurthala (PTU Main Campus), Jalandhar, Punjab, India

Accepted 10 Nov 2014, Available online 01 Dec 2014, **Vol.4, No.6 (Dec 2014)**

Abstract

Wireless sensor network(WSN) is collection of sensor nodes and it is self configuring, dynamically changing, multi hop wireless network which forms a communication network via multi hop wireless network connection. Nodes in the network communicate with another node if it lies within the transmission range. Every node act as source and router in the network .Such sensor network is used in wide range of applications. In WSN security is very challenging and growing research field because of some kind of novel attacks i.e clone attack because of its dynamic nature. clone avoidance is one of the key problem in WSNs as clone avoidance in network is essential for security of sensor nodes ,data confidentiality, and for better performance of the network. The proposed approach uses the concept of threshold to avoid clone attack in the network, the key idea is to use sensor nodes crosses the maximum threshold do not consider in the path. The proposed approach (TBCA-AODV) is able to avoid clone nodes from the path and will increase the network performance. The simulation done in ns-2 and the proposed algorithm is compared with existing AODV and AODV with Clone attack and is performance better in case of throughput and packet delivery ratio of the network.

Keywords: *Wireless sensor network , clone nodes ,threshold, Avoidance of Clone node*

1. Introduction

A wireless sensor network consists of spatially tribute autonomous sensors to monitor physical or environmental conditions. Wireless sensor networks can be deployed in harsh environments to fulfill both military and civil applications. A Wireless Sensor Network is a collection of sensors with limited resources that collaborate to achieve a common goal. They are often unattended and prone to different kinds of novel attacks due to their operating nature. Due to their operating nature there are some kinds of novel attacks are possible in WSN known as Black hole attack, Worm hole, Sybil attack etc. six different inoculants system having the same quantity and on the same base chemical composition of iron melt.

A. Cloning Attack

The most common attack in WSN is clone attack. Avoidance of clone attack is more challenging issue in WSN. An adversary may captured sensors and deploy them in the network to launch a variety of malicious activities. This is referred to as clone attack. Replicating a node implies cloning the node ID and all the cryptographic material that is associated to that ID. Hence clone node can communicate with other as legitimate nodes and being identified as a legitimate one .Once cloned nodes are deployed in the network , the adversary can use them in several malicious ways and accept data packets from other legitimate nodes and drop these packets in the network.. The clone attack is very convenient for an adversary. Moreover, avoidance of such attack is very challenging, since a clone cannot be easily avoid and detected with only local topology knowledge.

B. AODV

AODV is an on-demand, single path, loop-free distance vector protocol. It combines the on-demand route discovery mechanism in DSR with the concept of destination sequence numbers from DSDV. However, unlike DSR which uses source routing, AODV takes a hop-by-hop routing approach.

1. Route Discovery and Maintenance

1.1 Route Discovery

In on-demand protocols, route discovery procedure is used by nodes to obtain routes on an ‘as needed’ basis. In AODV, route discovery works as follows. Whenever a traffic source needs a route to a destination, it initiates a route discovery by flooding a route request (RREQ) for the destination in the network and then waits for a route reply (RREP). When an intermediate node receives the first copy of a RREQ packet, it sets up a reverse path to the source using the previous hop of the RREQ as the next hop on the reverse path. In addition, if

*Correspondinh author: **Sharanjit Kaur**

there is a valid route available for the destination, it unicast a RREP back to the source via the reverse path; otherwise, it re-broadcasts the RREQ packet. Duplicate copies of the RREQ are immediately discarded upon reception at every node. The destination on receiving the first copy of a RREQ packet forms a reverse path in the same way as the intermediate nodes; it also uni cast a RREP back to the source along the reverse path. As the RREP proceeds towards the source, it establishes a forward path to the destination at each hop.

1.2 Route Maintenance

Route maintenance is done by means of route error (RERR) packets. When an intermediate node detects link failure (via a link-layer feedback, e.g.), it generates a RERR packet. The RERR propagates towards all traffic sources having a route via the failed link, and erases all broken routes on the way. A source upon receiving the RERR initiates a new route discovery if it still needs the route. Apart from this route maintenance mechanism, AODV also has a timer-based mechanism to purge stale routes.

The graphs must be properly drawn in MS excel. Please note that all the legends should be drawn in the MS excel single file. They are not to be inserted in MS Word which will affect the formatting of the template. Care should also be taken to keep the font as Times New Roman. As the default font in Excel is Calibri. So the graphs by default take it. The authors are required to keep the font as Times New Roman.

2. Literature Survey

Kanagavalli.N *et al*. (2013) proposed scheme is based on mobile sink server which determines the parameters such as traffic, time and bandwidth of all the mobile sink. An uncompromised mobile node should never move at speeds in excess of the system-configured maximum speed. If the node misbehaves it revokes and assign MS randomly. Thus the replication of node and its identity can be resolved. Hence data collection can be done in secure manner.

Lou Yanxiang, *et al*. (2012) Node replication attack is a great threat to the security of wireless sensor networks. Existing detection protocols fail to hold in mobile WSNs, or if nodes collude to subvert the detection protocol. In this paper, a novel scheme for detecting node clone attacks in mobile WSNs, namely the Single Hop Detection (SHD) protocol, which is fully distributed in that all communication happens between single hop neighbors, highly robust against node colluding, and highly efficient.

Animesh Patcha *et al*. (2003) The security of the ad hoc network routing protocols is still an open problem and deserves more research work. With the wide spread usage of the intemet as a shopping place, and the fast spread of wireless mobile units in the battle field and search and rescue missions, secure and reliable transfer of data especially audio and video data is the major challenge of the day. Therefore, there is strong need, now more than ever, for secure applications in the wireless world. This paper presents some extensions to the watchdog concept in scenarios where there is no a priori trust relationship between the nodes. Our initial results are promising and they indicate a solution towards the detection and isolation of malicious nodes in the network either working alone or colluding with other malicious nodes to bring the network down. They leads and design an efficient mechanism which can he smoothly integrated into current protocols to establish safe routes when false routing information is discovered. The results will help **us** design a more secure ad hoc routing protocol.

3. Problem Formulation

AODV is very efficient routing protocol used in WSN. As it is an on demand protocol paths are only created, when data transfer is needed but AODV do not provide any security measures and hence it is very vulnerable to different kind of attacks. Clone attack is one of the most common and harmful attack that can compromise the confidentiality and can reduce the Qos of routing protocol. There are different researches that can avoid the clone attack but they need to use authentication techniques or locations of every node in the network .Which has its own extra overhead.

Assumptions

- If node A can hear node B that implies that B can also hear node A.
- Threshold value is same for every node initially.
- The threshold is taken according to simulation time and data rate and mobility in the network , the value of threshold is 50.
- Clone has the property of dropping packets.

4. Threshold based Clone Avoidance Protocol

A. Proposed Algorithm

Although AODV is on demand routing protocol paths are only created , when data transfer is needed but AODV do not provide any security measures and hence it is very vulnerable to different kind of attacks. Clone attack is one of the most common and harmful attack that can compromise the confidentiality and can reduce the QoS of routing Protocol.

To overcome this problem we proposed and approach TBCA (Threshold Based Clone Avoidance AODV) the proposed approach works on the basis of the packet drop of the node. When any node drop packets in the path, neighboring nodes increment its drop counter. If the packet drop counter exceeds the THRESHOLD level in the network then that node is termed as clone node and an route error message (REER) is issued to the source.

```
If (path exits for destination)

{Distribute data among paths}

Else
{initiate route discovery}
```

```
Route discovery process

Send RREQ();     // RREQ->buffer is initiated 0

Packet Reception Route

Recv packet ()

{
If (pkt_Drop_Count> Threshold)
{
RT_Status = Down
Route error()
Send RREQ();
}
Recv REQ()
{
If (Threshod< node_drop_count)
{
Drop_request;
}
Else
{   // exiting AODV code
}
```

A source upon receiving the RERR initiates a new route discovery. Source initiates a new path discovery with RREQ.

The node send an REER message to source and source initiate a threshold to zero of every node and send RREQ message to discover a new path from source to destination and check threshold value of every node which comes in the path. The node in the path with high threshold is avoid from the path and clam as clone node in the network and data is send to next legitimate node in the path.

5. Simulation Results

The proposed protocol is experimented in the simulated environment with NS2. The MAC layer is based on IEEE 802.11 distributed coordination function.. The nodes are deploy randomly in area of 1000X1000 with 50 nodes. The simulation run is for 200 simulated seconds. The channel Propagation model we used is the 2-ray ground reflection model The threshold is of maximum 50 packets, threshold is variable that is count the dropped packets by a node. The interface queue is another queue that works between network and MAC layer and is taken 50 in the simulation scenarios. The detailed description of the simulation scenario is given in table 5.1

Table 5.1 Simulation Parameters

Parameters	Value
Dimension	1000x1000m2
Number of Nodes	50
Simulation Time	200s
Number of Connections	0-6(Variable)
Packet Size	1460 bytes
MAC Layer	IEEE 802.11
Threshold	50
Propagation Radio Model	Two Ray Ground
Physical Layer	Bandwidth 2Mb/s

5.1 Performance and Results

In order to investigate the performance of protocols, using the following performance metrics:

A. Performance Metrics

1. Packet Delivery Ratio

The packet delivery ratio in this simulation is defined as the ratio between the number of packets sent from constant bit rate sources (CBR, application layer) and the number of receiving packets by the CBR sink at destination. It specifies the packet loss rate, which limits the maximum throughput of the network.

2. Average End to End Delay

This metric represents an average end-to-end delay and indicates how long it took for a packet to travel from the source to the application layer of the destination. It includes all possible delay caused by buffering during route discovery latency, transmission delays at the MAC, queuing at interface queue, and propagation and transfer time. It is measured in seconds.

3. Throughput

Throughput is total packets success fully delivered to individual destination over total time.

5.2 Results and Discussions

Fig 1, 2 and 3 show the Comparison of AODV and AODV with Attack based on Packet Delivery Ratio, average end to end delay and throughput at threshold 50

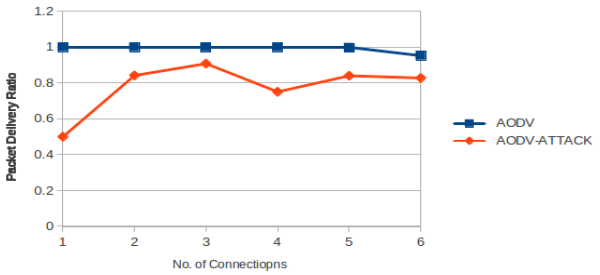

Fig. 1 Comparison of AODV and AODV with Attack based on Packet Delivery Ratio on threshold 50 .

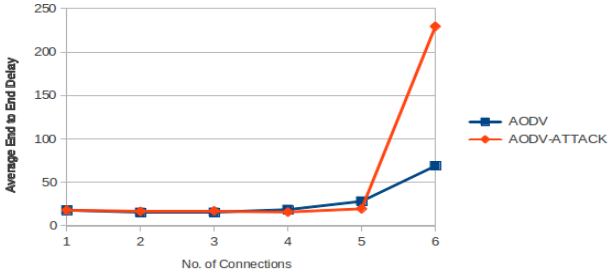

Fig. 2 Comparison of AODV and AODV with Attack based on Average End to End Delay on threshold 50.

The packet delivery ratio comes to very less than normal AODV protocol When clone node come in the path from source to destination because clone nodes drop maximum packets, so that the ratio of number of packet sent by source and number of packets received by destination is less than AODV.

The end to end delay of AODV and AODV with Clone Attack comes out larger than AODV because clone nodes drop maximum packets in path so very less packets are delivered at destination .Due to which the queue delay increases hence the total delay comes out to be large than AODV.

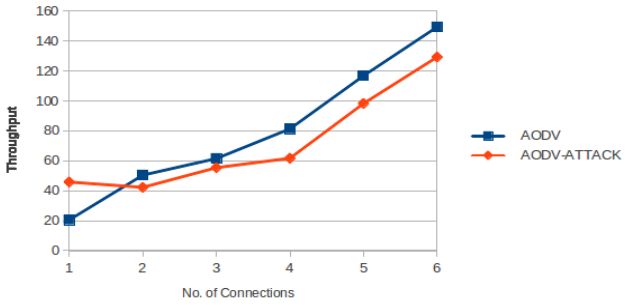

Fig. 3 Comparison of AODV and AODV with Attack based on Throughput on threshold 50

Throughput is total number of packets received per second. Clone nodes in the path has very bad effect on the throughput of the network as shown in figure 2 the Throughput of the network of AODV with attack are comes out less than AODV. Because clone nodes drop packets, they do not forward packets further in the path. Due to which very less packet received at destination hence overall throughput of the network decreases.

Fig 4, 5 and 6 show the Comparison of AODV_ATTACK and TBCA_AODV based on Packet Delivery Ratio, average end to end delay and throughput at threshold 50

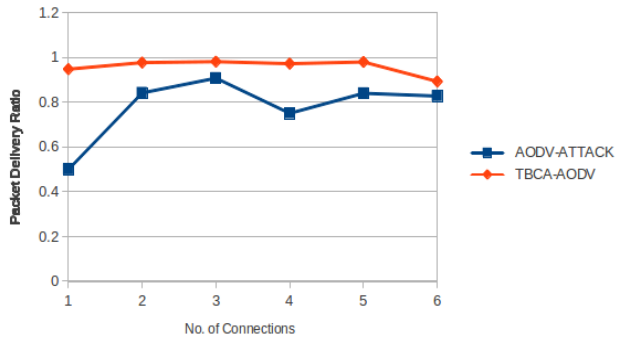

Fig. 4 Comparison of AODV- ATTACK and TBCA-AODV based on Packet Delivery Ratio on threshold 50.

Packet Delivery Ratio comes out large than AODV-ATTACK when clone nodes are avoid from the path using TBCA-AODV in the network maximum packets are delivered at destination, which increases the network performance.

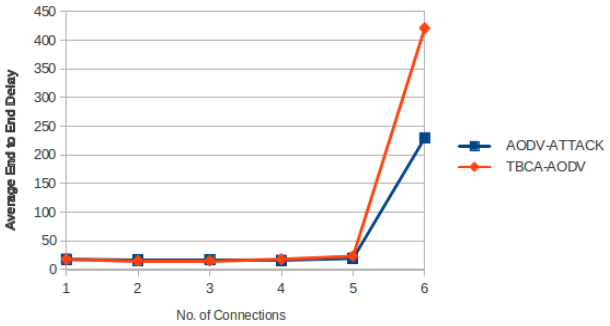

Fig. 5 Comparison of AODV- ATTACK and TBCA-AODV based on Average End to End Delay on threshold 50

Clone nodes drop maximum packets and avoid from the path so only delivered packets are considered in end to end delay due to which the average end to end delay of TBCA-AODV is increased.

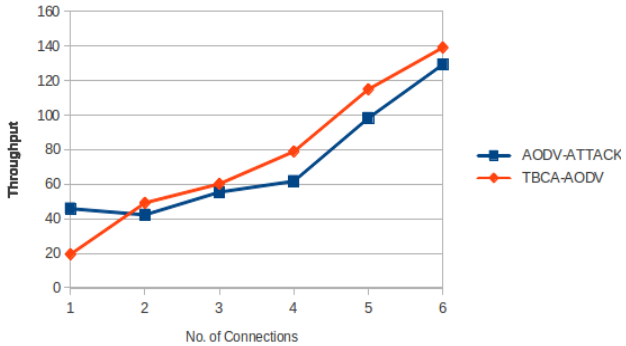

Fig. 6 Comparison of AODV- ATTACK and TBCA-AODV based on Throughput on threshold 50 .

The throughput are increased in TBCA-AODV because when we avoid clone nodes from the path in the network maximum packets are delivered at destination per second through which throughput of whole network is increased.

Fig 7, 8 and 9 show the comparison of AODV , AODV_ATTACK and TBCA_AODV and based on Packet Delivery Ratio, average end to end delay and throughput at threshold 50.

Graphs present the overall performance of the network in which throughput increases with TBCA_AODV and delay comes maximum.

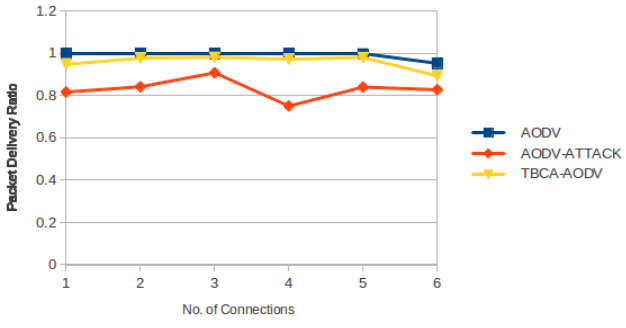

Fig. 7 Comparison of AODV , AODV- ATTACK and TBCA-AODV based on Packet Delivery Ratio on threshold 50.

Fig 7 shows the comparison between AODV, AODV-ATTACK and TBCA-AODV using threshold 50. The packet delivery ratio of TBCA-AODV is approximately same as AODV and large than AODV-ATTACK. Because TBCA-AODV do not accept those nodes whose threshold is greater than 50 so it avoid clone nodes from the path due to which less packets are drop in the path which increased the packet delivery ration of whole network.

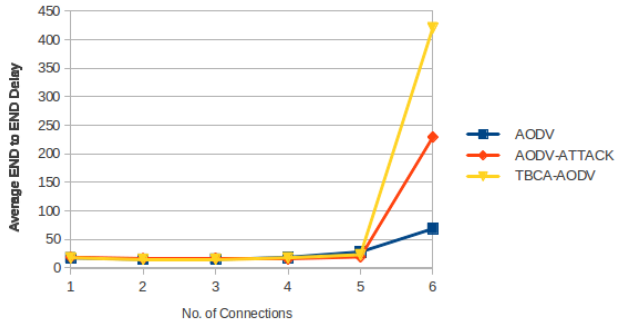

Fig. 8 Comparison of AODV- ATTACK and TBCA-AODV based on Average End to End Delay on threshold 50

Fig 8 illustrates the comparison of AODV, AODV-ATTACK and TBCA-AODV with respect to end to end delay when threshold is 50, when source send RREQ for new path discovery in the network delay increases and only delivered packets are considered in end to end delay.

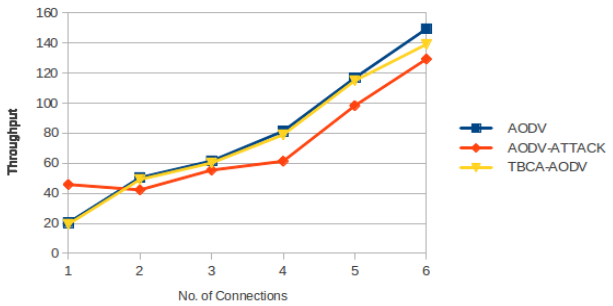

Fig. 9 Comparison of AODV- ATTACK and TBCA-AODV based on Throughput on threshold 50.

Fig 9 shows the throughput results at threshold 50.The throughput of TBCA-AODV is approximately same as AODV and greater than AODV-ATTACK. Due to clone avoidance from the path less packets are dropped in the path that is maximum number of packets are delivered per second at destination which increase the network throughput and increases the overall performance of the network.

Conclusions

A wireless sensor network is a collection of sensor nodes that communicate with each other by single and multi-hop radio network and maintain connectivity management without an existing infrastructure. These kind of networks are expected to have a very important role in military and civilian applications. To design clone attack avoidance protocol from the network to improve the network performance is a challenging issue. The goal of this research is provide new solution to avoid to clone nodes from the network and enhance the network performance.

The proposed Protocol ha following features:

1) The proposed protocol TBCA-AODV is single path routing protocol , which is able to avoid clone node from the path by using Threshold value.
2) It choose those nodes which has less threshold than maximum threshold , which helps to avoid clone nodes from the path.

The simulation is done in NS2 and comparison of existing AODV, AODV-ATTACK and TBCA-AODV is done by varying the number of connections by using maximum threshold 50.The proposed protocol surpassed the existing AODV by means of packet delivery ratio, average end to end delay and throughput. Based on the results the conclusion can be made that the proposed protocol is avoid clone attack in the network and hence enhance the performance of the network and ultimately provide us better throughput and packet delivery ratio in the network..

References

Jun Zheng , Wireless Sensor Networks .

Murali Pulivarthi ,Shafiulilah Shaik, M Lakshmi Bai, (November 2012), Detection of Clone attacks in Wireless Sensor Networks Using RED Protocol, International Journal of Engineering Research and Development e-ISSN: 2278-067X, p-ISSN: 2278-800X, www.ijerd.com Volume 4, Issue 7

C.Sujitha, V.Chandrasekar (March 2012) , Red Protocol For The Detection of Clone Attacks, International Journal of Communications and Engineering Volume 04 – No.4, Issue: 01.

Yanxiang Lou, Yong Zhang, Shengli Liu (2012), Single Hop Detection of Node Clone Attacks in Mobile Wireless Sensor Networks, International Workshop on Information and Electronics Engineering (IWIEE).

R. Brooks, P. Y. Govindaraju, M. Pirretti, N. Vijaykrishnan, and M. T. Kandemir (2007.), On the detection of clones in sensor networks using random key predistribution, IEEE Trans. Syst. Man Cybern., Nov.

Yingpei Zeng, Jiannong Cao (June 2010), Random-Walk Based Approach to Detect Clone Attacks in Wireless Sensor Networks, IEEE Journal On Selected Areas In Communications, VOL. 28, No. 5.

Kwantae Cho, Minho Jo (March 2013), Classification and Experimental Analysis for Clone Detection Approach in Wireless Sensor Networks, IEEE Systems Journal,

Zhijun Li (December 2013), On the Node Clone Detection in Wireless Sensor Networks, IEEE/ACM Transaction On Networking, VOL. 21, No. 6

Jun-Won Ho, Donggang Liu, Matthew Wright, Sajal K. Das (2009) Distributed Detection of Replicas with Deployment Knowledge in Wireless Sensor Networks, Department of Computer Science and Engineering The University of Texas at Arlington Arlington, March 23.

M.Conti ,R.DI Pietro, A.Spognardi (2013), Clone War: Distributed detection of clone Attacks inmobileWSNs, Department of Mathematics, Universitàdi Padova, , Journal of Computer and System Sciences

Stallings W. (2004), Data and Computer Communications, Prentice Hall, 7th Ed.

John A. Stankovic (June 2006) , Wireless Sensor Network ,

H. Wen, J. Luo L. Zhou (April 2011), Lightweight and effective detection scheme for node clone attack in wireless sensor networks, Published in IET Wireless Sensor Systems Received on 26th December 2010 Revised on 22nd

V. Manjula , Dr.C.Chellappan (March 2011) Replication Attack Mitigation for Static and Mobile WSN, International Journal of Network Security & Its Applications (IJNSA).

Z. Li and G. Gong (Oct. 2009), Randomly directed exploration: An efficient node clone detection protocol in wireless sensor networks, in Proc. IEEE Int. Conf. Mobile Adhoc Sensor Syst.,

B. Zhu, S. Setia, S. Jajodia, S. Roy, and L. Wang (Jul. 2010), Localized multicast: Efficient and distributed replica detection in large-scale sensor networks, IEEE Trans. Mobile Comput.,

Kai Bu, Xuan Liu, Jiaqing Luo, Bin Xiao (March 2013), Unreconciled Collisions Uncover Cloning Attacks in Anonymous RFID Systems, IEEE Transactions on information forensics and security

B. Parno, A. Perrig, and V. Gligor (May 2005), Distributed detection of node replication attacks in sensor networks, in Proc. IEEE Symp. Security Privacy.

Malek Ben Salem and Salvatore J. Stolfo (2002) ,Masquerade Attack Detection Using a Search-Behavior Modeling Approach, Computer Science Department Columbia University New York, USA

Issa Khalil, Saurabh Bagchi, Ness B. Shroff (2005.), LITEWORP: Detection and Isolation of the Wormhole Attack in Static Multihop Wireless Networks, Dependable Computing Systems Lab (DCSL) & Center for Wireless Systems and Applications School of Electrical & Computer Engineering, Purdue University.

Animesh Patcha and Amitabh Mishra ,Collaborative Security Architecture for Black Hole Attack Prevention in Mobile **Ad Hoc** Networks , Wireless Internet Networking Laboratory Department of Electrical and Computer Engineering, 2003 IEEE.