International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

A Modified Algorithm and Protocol for Replica Attack Prevention for Wireless Sensor Network

Dharmendra Singh Chouhan[1], Pritesh Jain[2]

[1]Pursuing M. Tech, Patel College of Science & Technology, Indore

[2]Associate Professor, Patel College of Science & Technology, Indore

Abstract: ***Wireless networks are achievement recognition to its height nowadays, because the users need wireless connectivity regardless of their geographic position. There's an increasing threat of attacks on the Wireless sensor Network (WSN). Node replication attack is one in all the security threat within which the traffic is redirected to such a node that really doesn't exist within the network. It's an analogy to the Replication within the universe within which things disappear. The node presents itself in such some way to the node that it will attack different nodes and networks knowing that it's the shortest path. WSNs should have a secure approach for transmission and communication that is kind of difficult and very important issue. So as to produce secure communication and transmission, research worker worked specifically on the security problems in WSNs, and lots of secure routing protocols and security measures inside the networks were proposed. The scope of this work is to review the effects of Replication attack in WSN exploitation (and prevention this attack exploitation security primarily based modified. Comparative analysis of Replication attack for each protocols is taken under consideration. The impact of Node Replication attack on the performance of WSN is evaluated searching for that protocol is additional vulnerable to the attack and the way abundant is that the impact of the attack on each protocols. The measurements were taken within the light of packet delivery ratio, throughput, end-to-end delay and residual energy. Simulation is completed in Network simulator tool two (NS-2).***

Keywords: WSN, Replication attack, AODV Routing Protocols, NS-2.35

1. Introduction

In recent years, advance in micro-electro-mechanical systems (MEMS) that are the integrations of mechanical parts, sensors, actuators and electronics on a typical silicon substrate through small fabrication technology and have enabled low-cost and low-power in electronics and wireless communication technology enabled small sensor nodes to communicate in short distance. Wireless sensor Networks (WSNs) comprise various small sensor nodes that are deployed in spatially distributed terrain. Every sensor node is endowed with a restricted amount of process, however once coordinated with the knowledge from different nodes, they need the flexibility to measure the given physical atmosphere in great details or to execute a task with advanced functions.

Hence, a sensor network may be represented as a set of sensor nodes that coordinate with one another to perform some specific actions. Since every sensor node is fitted with an on-board processor, sensor nodes use their process abilities to seek out simple computations and transmit solely the required information. These features permit the sensor networks to use in several applications, like military, security and atmosphere. Wireless sensor networks can also be deployed within the ways in which the wired sensor system can't be deployed such as within the chemical environments that are inaccessible by humans.

2. Classification of Protocols

Routing techniques are needed for sending information between sensor nodes and also the base stations for communication. Completely different routing protocols are proposed for wireless sensor network. These protocols are classified consistent with completely different parameters. Protocols will be classified as supported their mode of functioning and kind of target applications.

- Proactive.
- Reactive
- Hybrid

In a proactive protocol the nodes start their sensors and transmitters, sense the atmosphere and transmit the information to a bus through the predefined route. The Low Energy adaptive clustering hierarchy protocol (AODV) utilizes this kind of protocol. In case of a reactive protocol if there are unexpected changes within the sensed attribute on the far side some pre-determined threshold value, the nodes immediately react. This kind of protocol is employed in time important applications. The threshold sensitive Energy efficient sensor Network (TEEN) [8] is an example of a reactive protocol.

Hybrid protocols like adaptive Periodic teen (APTEEN) incorporate each proactive and reactive ideas [9]. They initial compute all routes so improve the routes at the time of routing. Further, consistent with the participation type of the nodes routing protocols may be classified as direct communication, flat and clustering protocols.

AODV (Ad-hoc on Demand Distance Vector): In AODV, nodes discover routes in request-response cycles. A node requests a route to a destination by broadcasting [2] associate RREQ message to any or all or any its neighbours. Once a node receives associate RREQ message however doesn't have a route to the requested destination, it successively broadcasts the RREQ message. The requesting node which can be used to forward ulterior responses to the current RREQ. This method repeats until the RREQ reaches

a node that incorporates a legitimate route to the destination. These nodes (which are the destination itself) respond with associate RREP message. This RREP is uni-cast on the reverse-routes of the intermediate nodes till it reaches the first requesting node. Thus, at the tip of this request-response cycle a pair of ray route is established between the requesting node and therefore the destination. Once a node loses property to its next hop, the node invalidates its route by used associate RERR to any or all or any nodes that most likely received its RREP.

3. Proposed Protocols

RAODV (Replica Ad-hoc on Demand Distance Vector): In this work we tend to focus our attention to 1 special active attack known as replica attack. In replica attack the router can advertise within the network that it's a recent route to the destination and at the moment might drop all the packets that it receives. Here, Intermediate nodes will cause inconsistent , If the source sequence number is recent and intermediate node have value above a source node then malicious node benefit of this high sequence number and sending pretend Route reply to the supply while not having actual route and drops all the receiving packets. It provides serious the damage. In replica attack, a particular malicious node that doesn't exist within the network, redirected all network traffics. Because traffics disappear into the special node as if the matter disappears into replica in universe.

SAODV (Source Ad-hoc on Demand Distance Vector): Route discovery process: once a source node needs to start data transmission with another node within the network, it checks its routing cache. If route is not available to the destination in its cache or a route is expired, it broadcast RREQ. Once the destination is found or any intermediate node that has fresh enough route to the final node, RREP is generated. Once the source node receives the RREP it updates its caches and therefore the traffic is routed through the route.Nodes receive sensed information, aggregate the information to remove redundancy and fusion processes are distributed and data is send to the sink (or Base Station). Therefore AODV will increase network time period by decreasing network energy consumption, and reducing variety of communication messages by information aggregation and fusion. The method of formation of clusters in SAODV may be a Source Adhoc routing protocol supported AODV.

4. Implementation and Result

In this work, the random way point static model is used for the simulation of WSN routing protocols. The source-destination pairs are spread randomly over the network where the point to point link is established between them.

In this work UDP agent with CBR traffic is used with 40 packet size and 10kbps rate used for the transmission. The simulation configuration for static nodes consists of many network components and simulation parameters that are shown in the table in detail.

A. Network Simulation

Generally network simulators try to model the real world networks. The principle idea is that if a system can be modelled, then futures of the model can be changed and the corresponding results can be analysed. Following features are provided by simulator.

Table 1: Simulation parameter

Simulation TOOL	Network Simulator-2.35
IEEE Scenario	WSN (802.15.4)
Static Model	Two Ray Ground
Number Of Nodes	30,60,80,120
Node Movement speed	Static network
Traffic Type	UDP
Antenna	Omni Directional Antenna
MAC Layer	IEEE 802.15.4
Routing Protocols	AODV , RAODV , SAODV
Queue Limit	50 packets
Simulation Area(in meter)	2000*2000
Queue type	Drop tail
Channel	Wireless Channel

The following metrics are used in this work for the detection and prevention of the node replication attack with AODV routing protocol.

Packet Delivery Ratio

This is the fraction of the data packets received by the destination to those sent by the source. This classifies the ability of the protocol to discover routes.

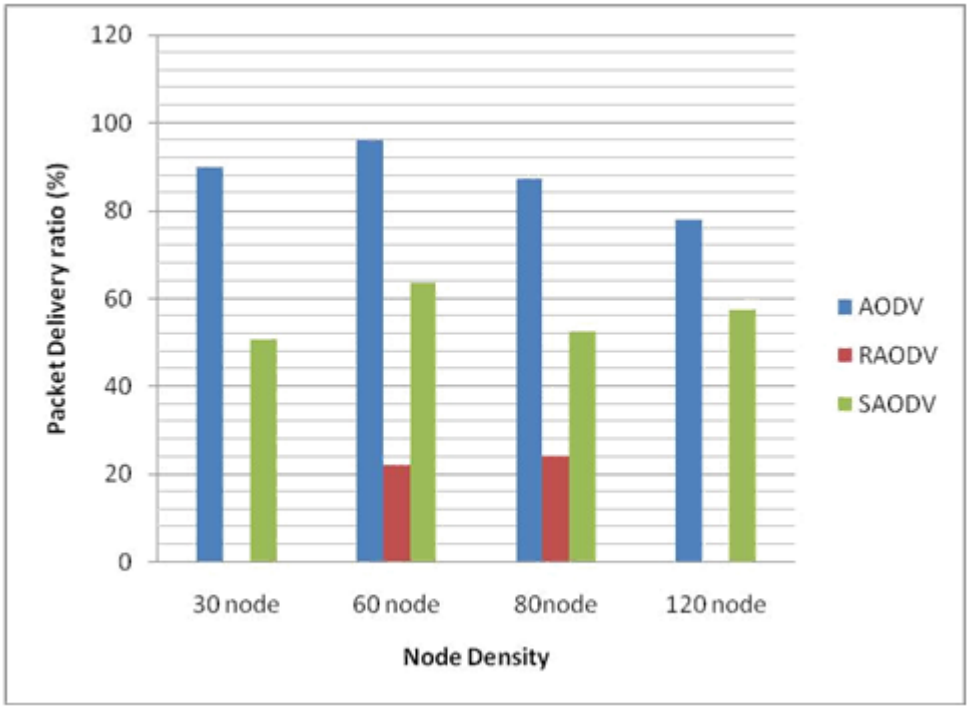

Figure 1: Packet Delivery Ratio under AODV, RAODV and SAODV

Analysis of Packet Delivery Ratio: The fig shows the effect to the packet delivery ratio (PDR) measured for the AODV, RAODV, SAODV protocols when the node Density is increased. It is measured that the packet delivery ratio dramatically decreases for RAODV.

B. End to End Delay

This is the average delay between the sending of the data packet by the source and its receipt at the corresponding receiver. This includes all the delays caused during route acquisition, buffering and processing at intermediate nodes.

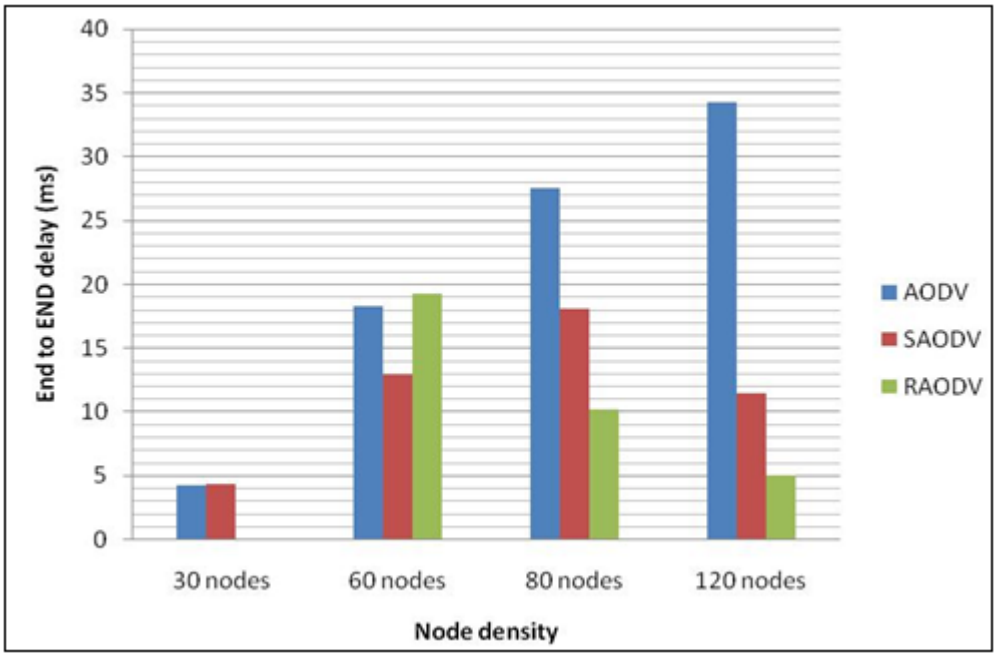

Figure 2: End to End Delay under AODV, RAODV and SAODV

C. Throughput

There are two representations of throughput; one is the amount of data transferred over the period of time expressed in kbps. The other is the packet delivery percentage obtained from a ratio of the number of data packets sent and the number of data packets received.

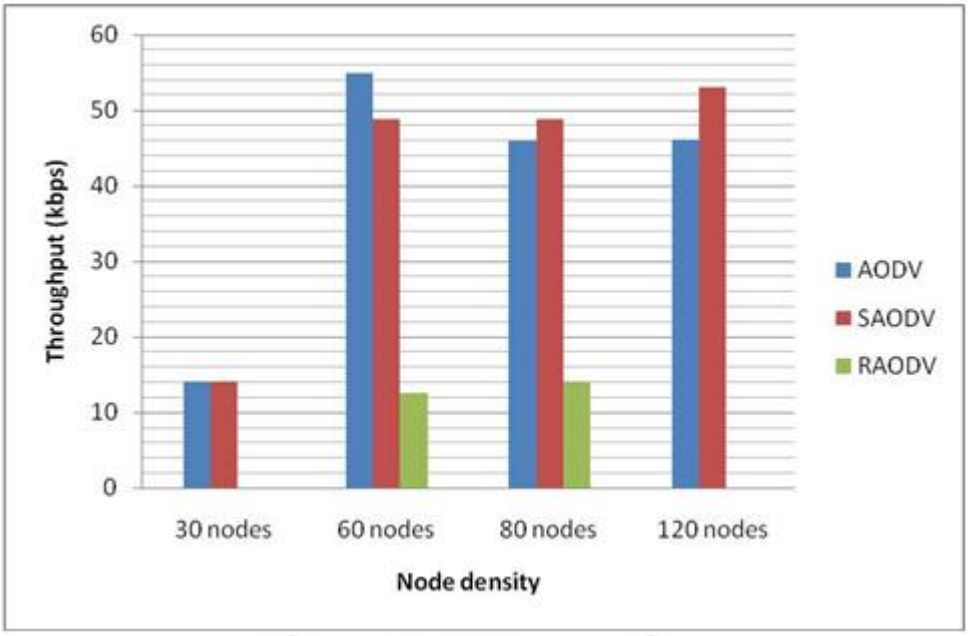

Figure 3: Throughput under AODV, RAODV and SAODV

Analysis of Throughput:
Higher value of throughput ensures large number of data packets successfully received at the Destination node. From the above figure it analysed that under replica node attack the Throughput of SAODV is more nearly similar to normal AODV, as compared to AODV under replica node attack. Figure shows with increasing the number of nodes, throughput of network also increases.

5. Conclusion

This work carried out the detailed analysis of Replication attack prevention and its detection through the trust mechanism with AODV routing protocol which is simulated by NS-2 for WSN on the basis of different performance metrics viz. packet delivery ratio, end to end delay, residual energy and average throughput. These performance metrics are analysed for the AODV, RAODV and SAODV routing protocols by varying the node density for fixed network. Simulation of routing protocols provides the facility to select a good environment for routing and gives the knowledge how to use routing schemes in attack network. Simulation results show that, as the density of nodes increases in the network, the performance of the routing protocols decreases. Attacker nodes affect the performance of routing protocols most as path break increases. According to simulation results as the RAODV prevent through the SAODV, the packet delivery ratio, Throughput and End to End delay of routing protocol increases as compare to the detection of RAODV through the SAODV.

References

[1] P. Jeyabharathi, A. Sivasankari, M. Maharasi, “An Efficient Security Mechanism for Data Reporting In Wireless Sensor Networks” www.ijera.com Vol. 3, Issue 5, Sep-Oct 2013, pp.333-338
[2] Dong-Wook Kim, Wan-Seon Lim, and Young-Joo Suh, "A Multichannel Relay MAC Protocol for IEEE 802.11 Wireless LANs," International Journal of Communication Systems.
[3] Tarun Anand Malik , “Target tracking in wireless sensor networks” Maharishi Dayanand University (India) May, 2005
[4] Shilpi Agarwal, Rajeshwar Lal Dua and Ravi Gupta, “Performance evaluation of parameters Using DSR Routing Protocol in WSNs” International Journal of Advanced Research in Computer Science and Software Engineering 2 (8),August- 2012, pp. 1-6
[5] Devendra Prasad and Reema Goyal “Secure and Energy Efficient Centralized Routing Protocol for Hierarchical WSN” www.ijerd.comVolume 2, Issue 9 (August 2012), PP. 41-45
[6] Amer A. Al-Rahayfeh, Muder M. Almi’ani, and Abdelshakour A. Abuzneid, “parameterized effect of transmission-range on loss of network connectivity of wireless sensor networks” International Journal of Wireless & MobileNetworks (IJWMN), Vol.2, No.3, August 2010
[7] Mohsin Raza Jafri, Nadeem Javaid, Akmal Javaid, Zahoor Ali Khan, “Maximizing the Lifetime of Multi-chain PEGASIS using Sink Mobility”, Mar 18, 2013
[8] Ouadoudi Zytoune1 and Driss Aboutajdine, “A Lifetime Extension Protocol for Data Gathering in Wireless Sensor Networks” , International Journal of Innovation and Applied Studies ISSN 2028-9324 Vol. 4 No. 3 Nov. 2013, pp. 477-482
[9] Samia A. Ali and Shreen K. Refaay, “Chain-Chain Based Routing Protocol”,IJCSI International Journal of ComputerScience Issues, Vol. 8, Issue 3, No. 2, May 2011.
[10] Tarun Gulati and sunita Rani, “An improved pegasis protocol to enhance energy utilization in WSN”, International Manuscript ID: ISSN2249054X-V2I3M7-052012 VOLUME 2 ISSUE 3 May 2012.
[11] Nisha Sarwade, Sanjay Waware and Pallavi Gangurde, “A Review of Power Efficient Hierarchical Routing Protocols in Wireless Sensor Networks”, International Journal of Engineering Researchand Applications (IJERA) Vol. 2,Issue 2, Mar-Apr 2012.

[12] Rathna. R and Sivasubramanian, "Improving energy efficiency in wireless sensor networks through scheduling and routing", International Journal Of Advanced Smart Sensor Network Systems (IJASSN), Vol 2, No.1, January 2012.
[13] Razieh Sheikhpour, Sam Jabbehdari and Ahmad khademzadeh, "A Cluster-Chain based Routing Protocol for Balancing Energy Consumption in Wireless Sensor Networks ", International Journal of Multimedia and UbiquitousEngineering Vol. 7, No. 2, April, 2012
[14] Se-Jung Lim and Myong-Soon Park, "Research Article Energy-Efficient Chain Formation Algorithm for Data Gathering in Wireless Sensor Networks", International Journal of Distributed Sensor Networks Volume 2012, ArticleID 843413, 9 pages doi:10.1155/2012/843413 July 2012
[15] Mohammad soleimani, mohammad ghasemzadeh and mehdi agha sarram, "A New cluster based routing protocol for prolonging network lifetime in wireless networks", Middle-East journal of scientific Research7(6) 884-890 2011
[16] Ge´rard Chalhoub and Michel Misson, "Cluster-tree based energy efficient protocol for wireless sensor networks", Institute of Electrical and Electronics, NOV-2010.
[17] Young-Long Chen, Jia-Sheng Lin, Yung-Fa Huang, Fu-Kai Cheung and Jen-Yung Lin, "Energy Efficiency of a Chain-Based Scheme with Intra-Grid in Wireless Sensor Networks", 2010 International Symposium on Computer,Communication, Control and Automation,VOL.2, ,2010, pp.484-487.
[18] Cong Wang1 and Cuirong Wang, "A Concentric Data Aggregation Model in Wireless Sensor Network ,"PIERSProceedings, Beijing, China, March 23–27, 2009
[19] Se-Jung Lim and Myong-Soon Park, "Research Article Energy-Efficient Chain Formation Algorithm for DataGathering in Wireless Sensor Networks", International Journal of Distributed Sensor Networks Volume 2012, ArticleID 843413, 9 pages doi:10.1155/2012/843413 July 2012.
[20] Mohammad soleimani, mohammad ghasemzadeh and mehdi agha sarram, "A New cluster based routing protocol for prolonging network lifetime in wireless networks", Middle-East journal of scientific Research7 (6) 884-890 2011.
[21] Ge´rard Chalhoub and Michel Misson, "Cluster-tree based energy efficient protocol for wireless sensor networks", Institute of Electrical and Electronics Engineers, Nov-2010.
[22] Young-Long Chen, Jia-Sheng Lin, Yung-Fa Huang, Fu-Kai Cheung and Jen-Yung Lin, "Energy Efficiency of a Chain-Based Scheme with Intra-Grid in Wireless Sensor Networks", 2010 International Symposium on Computer,Communication, Control and Automation,VOL.2, ,2010, pp.484-487.
[23] Cong Wang1 and CuirongWang, "A Concentric Data Aggregation Model in Wireless Sensor Network ,"PIERSProceedings, Beijing, China, March 23–27, 2009