International Journal of Science Engineering and Advance Technology

Virus Attack Identification And Representation In Sensor Network

[1]Chintha Venkata Ramana,[2]Mr.B.P.N.Madhu Kumar
[1]M.tech Student,[2]Associate Professor in CSE Department,
B V C Engineering College,Odalarevu, Andhra Pradesh, India.

***Abstract*:**

Clusters consist of circulated sensors and motor that interact with each other via wireless network. The use of open wireless intermediate and unattended deployment leaves these systems vulnerable to intelligent adversary whose goal is to disrupt the system performance. Here we study the virus attack on a networked control system, in which an opponent establishes a link between two physically different areas of the network by using either high-gain antennas, as in the out of band, or colluding network nodes as in the in-band virus. Virus allow the adversary to violate the timing constraints of real-time control systems by first creating low latency links, which attack network traffic, and then delaying or dropping packets.

The requester and responder in between the data sending through a transport channel then data can be destroyed or modified, so to avoid those problems we are proposing a new system by using NS2 features. Our approach is based on the analysis of the two-hop neighbours forwarding Route Reply packet. To check the validity of the sender, a unique key between the individual sensor node and the base station is required to be generated by suitable scheme. In our proposed work detection of virus attack is done through observing the performance of the route under various metrics those are packet delivery fraction, end-to-end delay and throughput. If the route having high end-to-end delay and low packet delivery fraction and low throughput that route must contains a virus nodes. So we can avoid those routes in the routing.

KEYWORDS:

Wireless Sensor Network, Sensor Nodes, Base Station, Virus

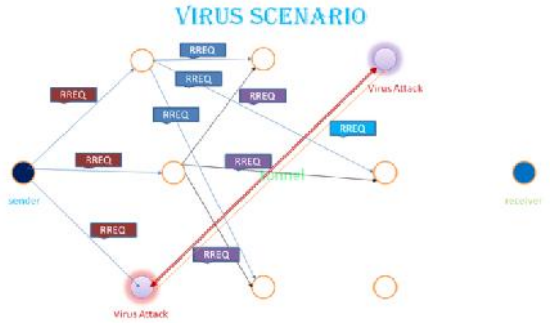


Figure-1: Virus attack

1. INTRODUCTION:

Wireless Sensor system (WSN) is regularly consisting of generously large number of inhibited sensor apparatus which are communicated over the wireless radio. The important applications of WSN include ecological monitoring, individual healthcare, challenger monitoring, etc. Sometimes the perceptive information is transferred to the target node from opening to end an disturbed medium. Thus, WSN can be facilely assailed by Denial-of-Service (DoS) attacks, which cause data loss along with extremely immense energy expenses. Therefore, acquiring the links is leading in manipulative a sensor network. Collider attack is a suppositious subway alliance two dissimilar outlets in space in such an approach that a tour through the invader could take much less time than that in normal outer space time. In the same way, a colliding connection in WSN looks reliable to a shortcut between the sensors. Advances in wireless connections have enabled the development of low cost and low power wireless sensor networks (WSNs) . They usually are varied systems contain many small devices, called sensor nodes, that monitoring different environments in cooperative; i.e. sensors cooperate to each other and compose their local data to reach a global view of the environment; sensor nodes also can operate autonomously. In WSNs there are two other components, called "aggregation points" and "base stations" , which have more powerful resources than normal sensors. Virus attacks can cause severe damage to the route discovery mechanism used in many routing protocols. In a virus attack, the malicious nodes will tunnel the eavesdropped packets to a remote position in the network and retransmit them to generate bogus neighbor connections, thus support the routing protocols and weakening some security enhancements.

As demarcated in Figure-1, Since messages travel multiple hops it is important to have a high reliability on each link, otherwise the probability of a message transiting the entire network would be unacceptably low. Significant work is being done to identify reliable links using metrics such as received signal strength, link quality index which is based on “errors,” and packet delivery ratio. Significant empirical evidence indicates that packet delivery ratio is the best metric, but it can be expensive to collect. Empirical data also shows that many links in a

WSN are asymmetric, meaning that while node A can successfully transmit a message to node B, the reverse link from B to A may not be reliable. Asymmetric links are one reason MANET routing algorithms such as DSR and AODV do not work well in WSN because those protocols send a discovery message from source to destination and then use the reverse path for acknowledgements. This reverse path is not likely to be reliable due to the high occurrence of asymmetry found in WSN.. For example, the assailant can damage with the data messages, or selectively accelerative data Quite a few protected. protocols have been proposed in fiction to security against colliding attacks. Furthermost of them need either unnecessary hardware's or accurate synchronized clock. In this article, we present the model for how the virus or colliding attack is acting on the widely used WSN routing protocol AoDV and we test the working of AoDV in sensor environment through network simulator (NS2) with various performance metrics and reviled in graphs.

2. EXISTING WORK:

Taheri, Naderi, and Barekata in utilized leashes process with a heightened info-packet provider system to shrink extent costs of TESLA with Instantaneous Key Disclosure (tiK) protocol. Particularly in the situation of (ttM), Tran, Hung, and Lee brothers come from a method where every host is in place of pathway notes during communicating RREQ info-packet while accumulating RREP packet and time frame is also vital. Singh and Vaisla made an enhancement by swapping despatcher and receptor counter to employing answer and tender packet time rate.

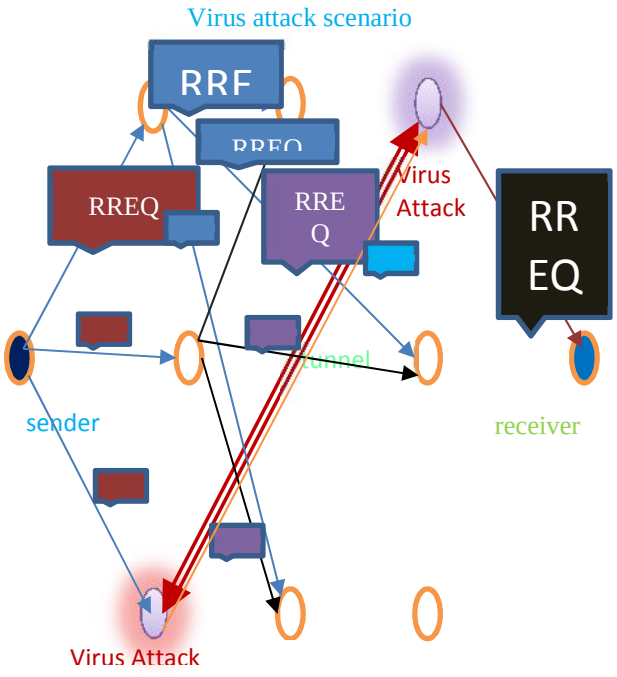


Figure-2: Throughput of AODV and WAODV

Evans and Hu provided that a scheme where the pinpointing antenna can crisscross details of neighbors by scrutinize localities of HeLLO messages and sensing besiders by verifiers. Remarkably, this organism can recognize a threat from an infiltrator by coming up with convinced brace of responsible keys, but help from hardware is a must and colliders with bogus besiders can be acknowledged with this procedure.

For finding virus attack risks, Khalil et.al had trivial counter measure (LITEWorP) with security hubs and in this way collide-attacker, LITEWorP goes out of sign from that opened hub just and builds possibilities of bars to understand this a convention called MOBIWorP, which had the capacity to dispose of undermining hubs by focal force from provincial or over-all. Chen, Lou, and Wang concocted a secured strategy for recognizing simplex and duplex virus dangers with a more extensive calculation for updating it to handle non-indistinguishable dispersal length of tangible hubs. Sadly, more than one virus can't be recognized along these lines.

3. IMPACT OF COLLIDING NODES ON AODV:

In this paper, we present the model for how the virus or colliding attack is acting on the widely used WSN routing protocol AoDV and we test the working of AoDV in sensor environment.

AODV is the best routing protocol is best fit over all other routing protocols for both Sensor and ad-hoc networks proved by most of the experiments. But it is also prone to various attacks in that most concentrating seeking attack is Virus attack. Here we show how virus attack is implemented on AODV in sensor networks.

AODV in WSN:

AODV is a variety of Destination-Sequenced Distance-Vector (DSDV) protocol which is on the whole taking into account DSDV and DSR. AODV working is completed with two strategic operations one is path disclosure and another is path upkeep. Route Detection: An initiator hub send a RREQ bundle to its neighboring hubs if no route is accessible for the coveted destination then the hub broadcasts the route ask for info-packet (RREQ) to achieve the destination. Route disclosure in AODV utilizes two pointers, for example, onward pointer and in opposite pointer. Onward pointers stay informed concerning the middle of the road hubs while message being sent to destination hub. At long last, when RREQ came to the destination hub, it then send back the RREP message to the source by means of the in the middle of hubs and the regressive pointer stays informed regarding the hubs. Route Maintenance: Three sorts of messages traded in the middle of source and destination, for

example, route mistake message, hello message and time out message.

Since messages travel multiple hops it is important to have a high reliability on each link, their wise the probability of a message transiting the entire network would be unacceptably low. Significant work is being done to identify reliable links using metrics such as received signal strength, link quality index which is based on “errors,” and packet delivery ratio. Significant empirical evidence indicates that packet delivery ratio is the best metric, but it can be expensive to collect. Empirical data also shows that many links in a WSN are asymmetric, meaning that while node A can successfully transmit a message to node B, the reverse link from B to A may not be reliable. Asymmetric links are one reason MANET routing algorithms such as DSR and AODV do not work well in WSN because those protocols send a discovery message from source to destination and then use the reverse path for acknowledgements. This reverse path is not likely to be reliable due to the high occurrence of asymmetry found in WSN.

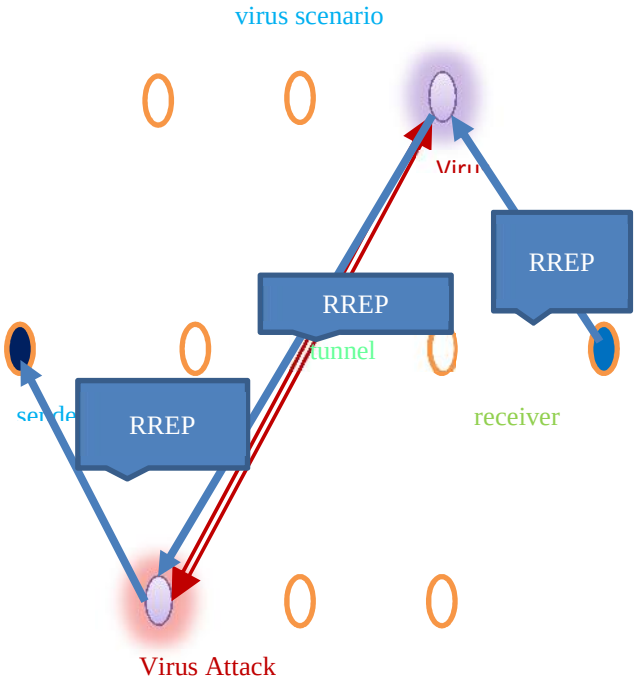


Figure-3: E2E Delay of AODV and WAODV

route error message guarantees that this message will be broadcast to all hubs in light of the fact that when a hub watches a fizzled path, it will engender this message to its upstream hubs towards source hub just. Hello message guarantees the onward and in opposite pointers from close.

Time out message ensures the erasure of connection when there is no movement for a sure measure of time in the middle of source and the objective hub. AODV directing is totally aggravated when there is a worm opening in the system.

Virus attack is launched during the route discovery process, a node wants to interconnect with other node normally this conversation is possible with shortest path which is provided by the AODV, that route is called as normal route. Virus attack is a colluding attack in which two nodes are collaboratively make this attack. Virus nodes comes into that route itself it advertise it is a shortest path then the route is established through the virus. Then result all the communication dropped selectively by the two virus nodes. So the performance of the network varies tremendously

4. PERFORMANCE ANALYSIS:

The performance is measured with network simulator 2. Here we use random way point mode is used to generate the traffic scenario. We perform simulation on normal AODV and virus AODV to illustrate the variation of network performance under various performance metrics.

Performance metrics:

Throughput: number of packets transferred from source to target in a particular time.

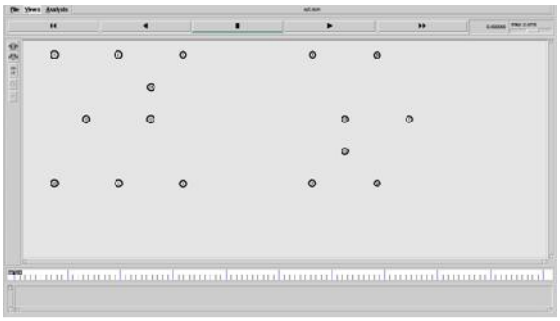
End To End Delay: the time taken to travel a data-pack from initiator to target.

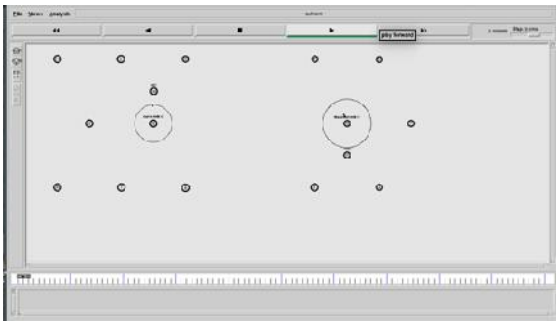
Hear figure shows that the comparison of AODV and worm hole AODV under throughput. Worm hole is a most hazardous attack where colliding nodes are in middle of the source and destination that is in the route and drops all the data packets. So the communication fails between the nodes. Through put means the number of data packets transferred from source host to target. Throughput of AODV is good. But under worm hole AODV the throughput decreased drastically.

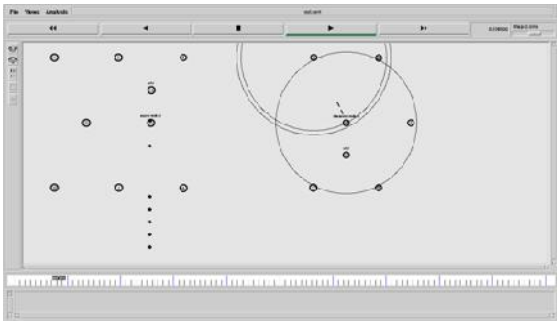
Hear figure shows that the comparison of end-to-end delay of normal AODV and virus AODV under end to end delay. Worm hole is a most hazardous attack where colliding nodes are in middle of the source and destination that is in the route and drops all the data packets. So the communication fails between the nodes. End-to-end delay the time taken to travel a packet from source to destination. Delay from one end to another end of AODV is high. Virus AODV having very high E2E delay compared to normal AODV.

The performance results shows that the comparison of AODV and Virus AODV with two performance metrics those are throughput and End-to-End delay. Virus decrease the network performance drastically proved by simulation results.

5. EXPERIMENTAL RESULTS







6. CONCLUSION:

In Sensors secure routing is most critical problem various kinds of attacks are possible sensor networks in those virus is a most focussed attack. It effects the performance of the network drastically. The performance results shows that the comparison of AODV and virus AODV with two performance metrics those are throughput and End-to-End delay. Virus decrease the network performance drastically proved by simulation results

REFERENCES:

[1] DemaAldhobaiban , Khaled Elleithy and LaialiAlmazaydeh “Prevention of Virus Attacks in Wireless Sensor Networks” 978-1-4799-7600-3/14 $31.00 © 2014 IEEEDOI 10.1109/AIMS.2014.57.

[2]Y. C. Hu, A. Perrig and D.B. Johnson, “Packet Leashes: A Defenseagainst Virus Attacks in Wireless Networks,” Wireless andMobile Communications. ICWMC’08, pp.13-18, 2008.

[3] M. Taheri, M. Naderi and M.Barekatain , "New Approach for Detection and defending the Virus Attacks in Wireless Ad HocNetworks," Proc. of IEEE International Conference on Communications, Vol. 10, pp. 3201–3205, June 2001.

[4] P.V. Tran , L. X. Hung ,Y.K. Lee, S. Y. Lee and H. Lee, "TTM: An Efficient Mechanism to Detect Virus Attacks in Wireless Ad-hoc Networks ," 4th IEEE conference on Consumer Communications and Networking Conference, pp. 593-598, 2007.

[5] A. Singh, K. S. Vaisla “A Mechanism for detecting Virus Attacks on Wireless Ad Hoc Network,” International Journal of Computer and Network Security, Vol. 2, no. 9, pp. 27-31, September 2010.

[6] L. Hu and D. Evans, “Using Directional Antennas to Prevent Virus Attacks,” Network and Distributed System Security Symposium (NDSS), February2004.

[7] I. Khalil, S. Bagchi and N. Shroff, “LITEWORP: A Light weight Counter measure for the Virus Attack in Multi hop Wireless Network , “International Conference on Dependable Systems and

Networks(DSN), pp.1-22, 2005.

[8] I .Khalil, S. Bagchi and N. Shroff , ” MOBIWORP: Mitigation of the Virus Attack in Mobile Multihop Wireless Networks,” international Conference on Depend able Systems and Networks(DSN), pp. 1-12, 2006.

[9] H. Chen, W. Lou, Z. Wang, “SLAW: Secure Localization against Virus Attacks Using Conflicting Sets,” Technical Report, The Hong Kong Poly technic University, pp.111, 2010.

[10] KritiPatidar and Vandana Dubey “Modification in Routing Mechanism of AODV for Defending Blackhole and Virus Attacks” 978-1-4799-3064-7/14/$31. 00©20 14 IEEE