Data Security in wireless Sensor Network using Multipath Randomized Dispersive Routes

Nagdev Amruthnath[1], Prathibhavani P M[2]

Abstract— Attacks are common in wireless sensor networks. In this paper we study the routing protocols to overcome the black holes formed by the attacks. We also discuss the problems that we have in our existing multipath routing and how to overcome the problems of our existing multi path routing by our proposed randomized random routing. In our proposed routing we generate random multi path routes and send the packets of information in these randomized multi path routes. By this proposed method it would be difficult for one to discover the routes in which the actual packets are being transmitted. Besides randomness the packets transmitted are highly dispersive and secure, making the bypass the black holes.

Index Terms— Attack, Black holes, Data Security, Multipath Network, Random routes, Security, Wireless sensor network.

1 Introduction

Wireless sensor networks are used to provide wireless communication infrastructure in sensor network. Sensor networks is the inter collection of several nodes. The applications of the wireless sensor network are increasing rapidly in the current scenario due to the fact that they are low cost solution for most of the real world problems. The infrastructure of the wireless sensor networks facilitates them in the use of real world applications. Hence security considerations in the wireless sensor network are very important.

The real threat in security of wireless sensor network is the problem of the compromised node and Denial-of-Service (DOS). These two problems would facilitate the creation of black hole in the network. The Compromised Node attack refers to the situation when an adversary physically compromises a subset of nodes to eavesdrop information Compromised node is formed when an adversary goes near a sensor node and compromises with that node. Due to the problem of compromised node the adversary can send the fabricated date to the user of the network and thus prevent him from receiving the actual packets. So, the user looses the actual packets and hence suffers badly due to this problem. Denial-of-Service is another severe problem due to which the user of the network misses the services provided by the network. In denial-of-service the adversary sends numerous requests to the server of the network and this gradually results in slowing down the speed in which network is operating and finally ends up with crashing the server. Due to this the users of the network would miss the service that is provided by the particular server. Black hole is a part of a network using which an adversary can attack the network or a particular route(s). In the black hole an adversary establishes his control over the subset of sensor nodes and reprograms the sensor nodes in such a way that, the nodes would fail to transmit the actual data packets and hence result in either failure of transmitting packets or transmits the fabricated packets to the respective destinations. Since the black hole problem would result in the manipulation of the actual data exchanged between source and destination, it is very serious problem that needs actual attention.

The existing multi path network is very much vulnerable to these types of attacks. Hence there is a demand in order to develop a very efficient approach to overcome these problems in the network.

In today's times security has become an important issue in networking. There has been a constant study for secure data transmissions over the network. Today, we have various cryptographic algorithms and routing protocols to achieve secure data transmission. But, these are still vulnerable to attacks. There are various security threats that exist in wireless sensor networks. Although the information is being encrypted and split in to packets by various cryptographic algorithms is a possibility that these are vulnerable to attacks.

In this paper, we are proposing a very efficient approach to overcome the security problems in the network. In our proposed methodology we are transmitting the packets using multipath randomized dispersive routes. Here, numerous randomized routes generated from source to destination. As a result of this it would become practically impossible for an adversary to take the entire information exchanged between the source and destination. Even though an adversary succeeds to capture the packets, he will only succeed in getting the part of the information not the entire information. Hence the data that is exchanged between the source and destination would be highly secure. When an adversary tries to capture the part of the information, the nodes in the network would sense this and changes the path of transmission.

2 Related Work

2.1 Review Stage

The most recently used multipath algorithms are Ad hoc On-demand Distance Vector Routing (AODV), Ad Hoc On-Demand Multipath Distance Vector Routing (AOMDV), Multicast Ad hoc On-demand Distance Vector Routing (MAODV). Several implementation of multipath routing are based on AODV. AODV is a simple flooding-based routing scheme assumes that each node is aware of its location and presents a greedy geometric routing algorithm. In AODV routing, when a source has data to transmit to a new destination, it broadcast a RREQ for that destination to its neighbors. A node on receiv-

International Journal of Scientific & Engineering Research Volume 5, Issue 1, January-2014
ISSN 2229-5518

ing the RREQ checks if it has not received the same request before using the ROUTE-ID. It is not the destination and does not have a current route to the destination, it rebroadcasts the RREQ and at same time backward route to the source is created. If the receiving node is the destination or has a current route to the destination, it generates a RREP. The RREP is uni cast in a hop-by-hop fashion to the source. As the RREP propagates, each intermediate node creates a route to the destination. When the source receives the RREP, it records the forward route to the destination and begins sending data. If multiple RREPs are received by the source, the route with the shortest hop count is chosen. In case a link break is detected, a RERR message is sent to the source of the data in a hop-by-hop fashion. As the RERR propagates towards the source, each intermediate node invalidates route to an unreachable destinations. When the source of the data receives the RERR, it invalidates the route and reinitiates route discovery. Sequence numbers in AODV play a key role in ensuring loop freedom and freshness of the route.

A. Proposed Protocol

The route discovery is done by using the steps of AODV routing algorithm on the basis of ROUTE-REQUEST, ROUTE-REPLY, ROUTE-ACK and ROUTE-ERR messages.

A. Route Discovery

For path discovery source node broadcast a route request (R-REQ) packet to all its neighbor nodes. The header of the RREQ packet contains the Sequence number and ROUTE-ID fields. The neighbor nodes then again rebroadcast the R-REQ packet to their neighbor nodes. So, a reverse path is generated between the source and the neighbor node. The nodes which already get a ROUTE-ID will discard all the next coming ROUTE-IDs in order to prevent the loop formation in the route. So, the R-REQ packets propagate in the network until the destination is found. When the destination is reached by the R-REQ packet reach to the destination, the destination node send a unicast R-REP message towards the source in a hop-by-hop fashion. So, a forward path is generated between the source node and the destination node.

3 Existing Approach

A. AODV

AODV stands for Ad Hoc On Demand Distance Vector. Each node in the network monitors the cost of the out going links. It is then periodically broadcasts the shortest routes to the neighboring nodes. In this protocol we use the RREQ (Route Request)packets and the RREP(Route Reply)packets to discover and maintain the shortest routes to the destination. When ever the source node has data packets to send, it sends RREQ packets to all the neighboring nodes. If the node is present in the route to the destination it sends a RREP packet to the source node. Thus by using the RREQ and RREP packets, a shortest route to the destination is discovered. Once the route is discovered, the data transmission can begin.

Every node maintains a Destination sequence number for each route entry. This number plays a very important role in the discovery of the routes to the destination. The destination sequence number is created by the destination for any route information which sends to requesting nodes, using destination sequence numbers ensures loop freedom and allows to know, to which of several routes is more "fresh". Given a choice between two routes to a destination a requesting node always selects the one with the greatest sequence number. Nodes that are part of active route may offer connectivity information by broadcasting periodically local hello messages (special RREP messages) to its immediate neighbors. If HELLO messages stop arriving from neighbor beyond some given time threshold the connection is assumed to be lost.

B. Existing network

Our existing network is a multipath network. Here during the first phase of the data transmission the best path is discovered for routing. Once the best route is discovered all the packets are transmitted over the network in the discovered shortest route. Our existing network is highly vulnerable to attacks. The attacks to our existing network include compromised node, denial of service (DOS attacks) and many more which in turn create black holes in our network. There have been various ideas proposed to overcome these issues like secrete sharing algorithms along with multiple routing algorithms. One of major attacks in a wireless sensor network is a compromised node attack. There is no exact or an accurate solution to overcome this attack. In this paper we propose an effective solution to overcome the problem of compromised node by randomized multi path network.

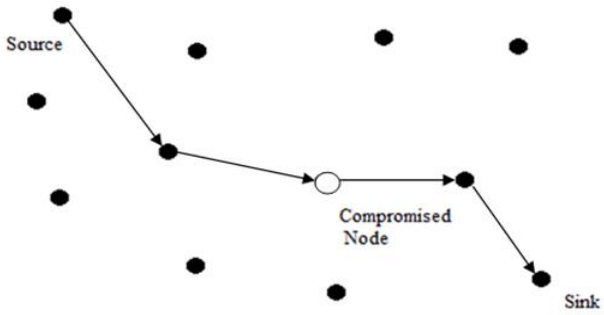


Figure 1. Multi path network with Compromised node

C. Problems of Existing Approach

The route between the source and the destination is predetermined; hence if the attacker finds out the route, the attacker can obtain all the data packets sent along the route, thus making this approach vulnerable to attackers.

In order to keep the routes alive the "HELLO" packets have exchanged constantly, this proves to be a hindrance as the energy is consumed without the transfer of data packets. Intermediate nodes can lead to inconsistent routes if the source sequence number is very old and the intermediate nodes have a higher but not the latest destination sequence number, thereby having stale entries. Also, multiple Route Reply packets in response to a single Route Request packet can lead to

International Journal of Scientific & Engineering Research Volume 5, Issue 1, January-2014
ISSN 2229-5518

heavy control overhead. Another disadvantage of AODV is unnecessary bandwidth consumption due to periodic beaconing

4 Proposed Approach

In this paper we propose randomized multipath routing to overcome the problem of compromised node attack in the network. Here, we focus mainly on data transmission. In this proposed network, instead of selecting a predefined path for the packet transmission we select the possible random routes in which the packets can be sent in the network. We send the packets in the multiple routes in the network. Hence ,in case of attack in our proposed network the attacker would not be able to find the source from which the packets are being sent and also will not be able to find the other random routes in which the remaining packets that are being sent in the network. In our proposed network, we disperse information packets in the network. The route that is used to send the packets will not be used again to send the packets during data transmission. Hence by our proposed randomized multipath network we achieve data security.

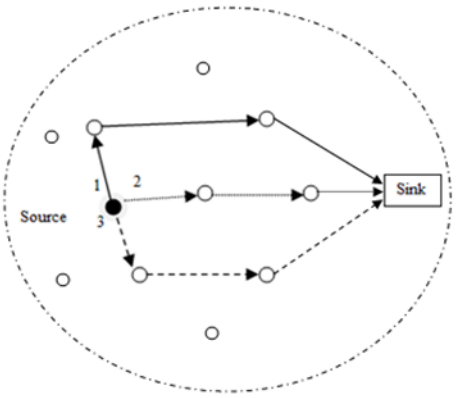


Figure 2. Randomized Multi Path Routing

A. Overview

As we have come across the problems of multipath routing in the following paper, we try to overcome the problems by randomized multipath delivery. In this paper we mainly focus on the packet transmission over the network. We try to disperse our packets over the network from source to destination. There is couple of Problems that has to be mainly focused upon. The key problems include looping, Packet transmission in the same route in the network when there are limited number of node and packets reaching the destination. To avoid looping in our network, we introduce a concept of Incremental distance packet transmission. In this when the packet is transmitted randomly in the network we send the packet such that it is sent farther from the source in each transmission of the packet. By this concept we have overcome the problem of looping in our proposed method. Our second problem is when there is limited number of nodes in the network; we send the packets in every possible path with compromising efficiency over security. Hence by this we are providing security of the data which is the main agenda of our paper. Finally, we come across the main problem in our proposed method, the packets reaching the destination. There is a possibility that the packet might not reach the destination in time due to dispersion of packets in the random multi path. To overcome the above issue, we add a TTL header to the packets (Time to Live). If the packet does not reach the destination within the time limit then the packet is dropped and an acknowledgement is sent from the destination to the source and the packet is resent to the destination. Hence, we are improving the security over the network.

B. Randomized Multipath Delivery

In our proposed approach we are trying to overcome the problems of multipath network by creating randomized routes. Initially the route is the shortest one to the destination. The next route would be the randomly selected route to the destination. The original information is broken into [M] number of shares using [T, M] threshold secret sharing algorithm. The source and destination nodes are determined and each node transmits a signal. By transmitting the signal every node realizes the neighboring nodes. The shortest distance between the source and destination is found and the transmission of data packet begins. Once the packet is sent, another random route is discovered and the next packet is sent to the destination. For every data packet received, an Acknowledgement packet is sent back.

Firstly, the information which needs to be transmitted is broken down into packets using the threshold secret share algorithm. Hello messages are used to detect and monitor links to neighbors. If Hello messages are used, each active node periodically broadcasts a Hello message to all its neighbors. Because nodes periodically send Hello messages, if a node fails to receive several Hello messages from a neighbor, a link break is detected. When a source has data to transmit to the destination, it broadcasts a Route Request (RREQ) for that destination. At each intermediate node, when a RREQ is received a route to the source is created. If the receiving random node has not received this RREQ before, it rebroadcasts the RREQ. If the receiving random node is the destination or has a current random route to the destination, it generates a Route Reply (RREP). As the RREP propagates, each intermediate node creates a route to the destination. When the source receives the RREP, it records this as a random route to the destination and begins sending data.

C. Algorithm

1. The source node 'S' broadcast the ROUTE-REQUEST to all its neighbors.

2. After getting the ROUTE-REQUEST the neighbor nodes check the ROUTE-ID, whether the ROUTEREQUEST has been received before.

3. If the ROUTE-REQUEST packet has been already received by the neighbor node, then it discards the packet.

4. Otherwise, a reverse path is established between the source and the neighbor node.

5. If this node is not the destination or having no path to the

International Journal of Scientific & Engineering Research Volume 5, Issue 1, January-2014
ISSN 2229-5518

destination, then

6. Repeat step 1 and onwards (neighbor node in place of source node)

7. When the ROUTE-REQUEST packet find the destination node or node having path to the destination, the destination node unicast the ROUTE-REPLY towards the source node.

8. When the ROUTE-REPLY packet reach to the source node following the path of intermediate nodes, the route is established in the reverse way i.e. from the destination to the source

9. The route is established, and the data packets can be sent through the established route.

D. Route Maintenance

The proposed protocol is used for the route-maintenance in the wireless network. After the route discovery process, we traverse the path in order to find the static nodes in the route. These static nodes are consists of buffers to store the necessary information and packets. If the static nodes are found in the route, then a buffer is attached to each static node in order to store the information regarding the static nodes and the packets in case of link failure. When the link between the two nodes are broken in the network that consist the static nodes, then predecessor node of the broken link send the ROUTE-ERR message towards the source. If there exist a static node in between the source node and the predecessor node then the message has to travel that much path only, i.e. the path between the predecessor node and the static node. Since the static node contains the route information (routing table) to the source, we need not to send the ROUTE-ERR message to the source. If the route is needed then route-caching or route-discovery (based on feasibility) process initiates from the static node not from the source. The buffer attached to the static node is used to store the data packets after the declaration of the broken link in order to prevent the packet loss. After the route-recovery the stored packets in the static node are sent to the destination.

5 Results and Simulation Studies

The operability and behavior of the routing protocol AODV in a wireless sensor network, the Network Simulator (NS-2) is installed on Linux OS. The table below shows the context of our simulation.

The following Figures shows the animated screenshots using NS-2, a set of nodes and random path generated between the source and destination respectively demonstrating the protocol functionality of AODV and random path generation using the following protocol.

TABLE 1
Simulation Setup Parameters

Network range	500x500 m
Transmission Range	250 m
Number of Nodes	10
Bandwidth	11 Mbps
Traffic Type	TCP
Packet size	512 Bytes

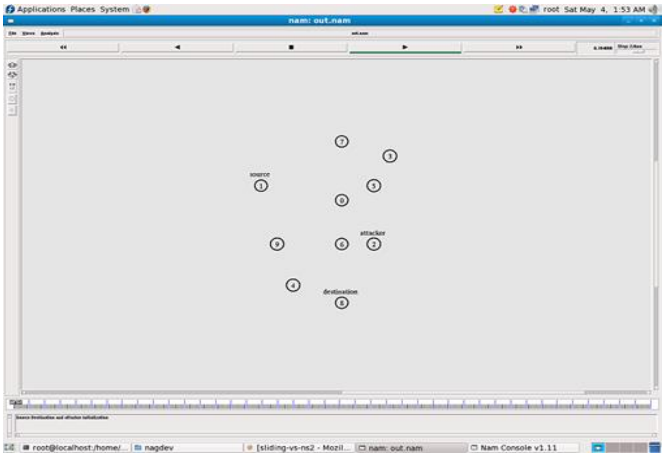


Figure 3 Network Topology

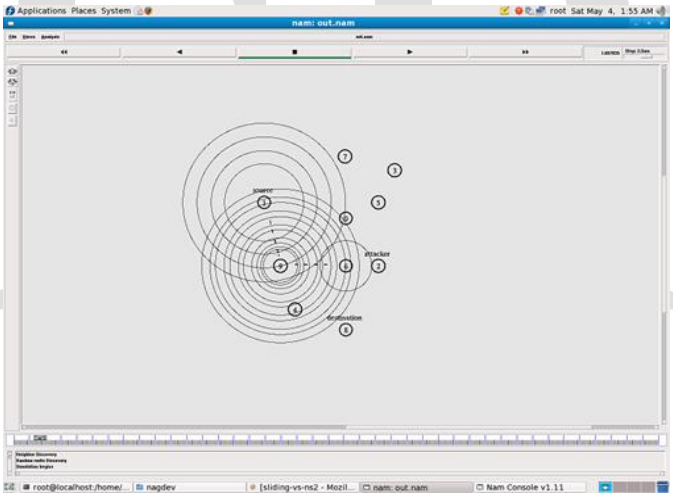


Figure 4 Random Routes 1

The Figure 3 represents the network topology. Our topology consists of 10 nodes. Our network includes a source, destination, attacker and intermediate nodes. In Figure 4 and Figure 5 we have generated a random route from node to destination. Here, we have observed 12 random routes to the destination. These random routes are unique.

The simulation result shows that the loss rate is increased when there is high mobility in the network. The dropping of packets may occur frequently, which leads to variations in the throughput of the network. The following graphs show the change in the number of random routes with respect to the increase in number of nodes and the change in throughput with respect to the increase in number of nodes.

International Journal of Scientific & Engineering Research Volume 5, Issue 1, January-2014
ISSN 2229-5518

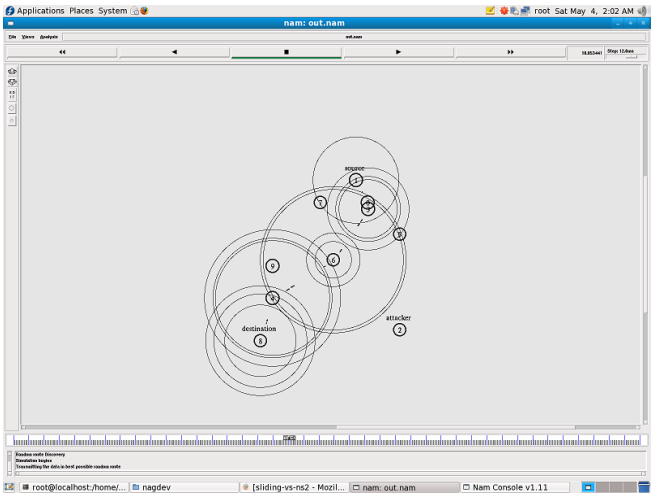
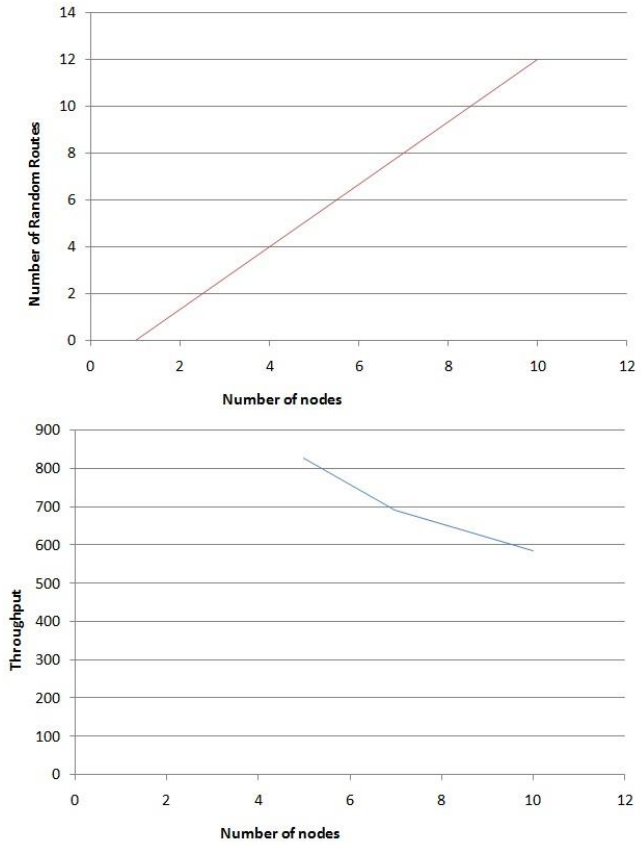


Figure 5 Random Route 2



By considering 10 nodes in the simulation with all the nodes being mobile and the simulation time considered for 40seconds the throughput observed is about 585.23 Kbps.

6 Conclusion

Our proposed method has shown the effectiveness of randomized dispersive routing in combating CN attacks. Our proposed method was compared against existing multi path network .The obtained results showed tremendous improvement of security performance.

Acknowledgment

The research was conducted as a part of our final year project and a project that was conducted for Old Dominion University under the guidance of Dr Ramesh Babu H S. Any opinions, findings, conclusions, or recommendations expressed in this paper are those of the author(s) and do not necessarily reflect our views.

References

[1] Tao Shu, Sisi Lui, and Marwan Krunz. Secure data Collection in Wireless Sensor Networks using Randomized Dispersive Routes. *IEEE Transactions on Mobile Computing*, pages 941 – 954, July 2012.

[2] Zehua Wang, Yuanzhu Peter Chen, Cheng Li, implementation of the AODV Routing Protocol in ns2 for Multi-hop Wireless Networks.

[3] Rachid Haboub and Mohammed Ouzzif, Secure Routing in WSN, *International Journal of Distributed and Parallel Systems*, Vol.2 No.6 November 2011.

[4] P. C. Lee, V. Misra, and D. Rubenstein. Distributed algorithms for secure multipath routing in attack-resistant networks. *IEEE/ACM Transactions on Networking*, 15(6):1490–1501, Dec. 2007.

[5] P. Papadimitratos and Z. J. Haas. Secure routing for mobile ad hoc networks. In *Proceedings of SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS)*, 2002.

[6] K.Vanaja, Dr. R. Umarani ,An Analysis of Single Path AODV Vs Multipath AOMDV on Link Break Using ns-2, *International Journal of Electronics and Computer Science Engineering*

[7] Tamer Nadeem, Ashok Agrawala, Performance of IEEE 802.11 based Wireless Sensor Networks in Noisy Environments