Secure Packet Transmission in Wireless Sensor Networks using Dynamic Routing Techniques

G. Ravi
Research Scholar
Dr. M.G.R Educational and
Research Institute University
Chennai - 600 095, India.

M. Mohamed Surputheen
Research Scholar
Dr. M.G.R Educational and
Research Institute University
Chennai - 600 095, India.

R. Srinivasan
PhD Dean, Research and PG
studies
RNS Institute of Technology
Bangalore– 560 061
India

ABSTRACT

Due to the unmanned nature of Wireless Sensor Networks, security becomes a key criterion when it comes to networks dealing with confidential data. Compromised node, Denial of Service (DoS) [1] attacks and Black-Holes/Sink-Holes [2] are the three key types of attacks in Sensor Networks. Classic routing algorithms use deterministic multipath routing schemes, where a predefined path exits between any two nodes. Once if the adversary acquires the routing algorithm it is possible to compute the route, making all information sent over these routes vulnerable to its attacks.
Our approach involves selecting intermediary nodes for each packet rather than sending the packets directly to the destination node. This way, the user initially disperses all the packets that are to be transmitted using a modified form of Backpressure algorithm [4] and then directs them to the destination node using SENCAST [5]. By following this method, most of the packets that are sent through a network have the probability of escaping black holes. Simulations show that our approach is much more effective in terms of security when compared to their deterministic counterparts.

Keywords

Wireless Sensor Network, Randomized Routing, Secret Sharing, Dispersive Routes

1. INTRODUCTION

1.1 Wireless Sensor Networks (WSN)

A Wireless Sensor Network consists of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants and to cooperatively pass their data through the network to a main location. Currently developed networks can function in both the directions, i.e. they can send and receive messages. Today sensor networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on.Energy is the scarcest resource of WSN nodes, and it determines the lifetime of WSNs. WSNs are meant to be deployed in large numbers in various environments, including remote and hostile regions, where ad-hoc communications are a key component. For this reason, algorithms and protocols need to address the following issues:

1. Lifetime maximization
2. Robustness and fault tolerance
3. Self-configuration

1.2 Motivations

Of the various possible security threats encountered by a WSN [3] & [13], we are interested in Compromised Node (CN) and Black-holes or Sink-holes attacks.

- **Compromised Node:** Compromised Node listens to or leaks information or manipulates information that pass through the network. This might lead to inappropriate or missing information in the base station.

- **Black-hole/Sink-hole Attack [2]:** In this attack, a malicious node acts as a black-hole to attract all the traffic in the sensor network. Then it says to the target nodes that it contains the high quality or shortest path to the base station. Once the malicious device has been able to insert itself between the communicating nodes (for example, sink and sensor node), it is able to do anything with the packets passing between them.

Both these attacks generate areas that can be used by the adversary to intercept information passed through it or modify the legitimate information passed to the base node. Since wireless sensor networks are mostly present in environments that are unattended, they are prone to attacks. Hence this becomes a serious problem when considering a wireless sensor network.

Conventional method of cryptography [1], [6] & [7] cannot be used to solve this problem, because if a node is compromised, the adversary can easily obtain the private and the public keys. Even if that is not possible, the user can still suck in all the packets transmitted to them hence creating a vacuum through which no packet can pass.

2. PROBLEM DEFINITION

The classic multipath routing approaches that are being used are vulnerable to attacks, mainly due to their deterministic nature. When using deterministic Routing, the attacker if gains access to a compromised node, can compromise the entire network because he can compute the routes based on obtained routing algorithm.

2.1 Backpressure Routing

The Backpressure Routing algorithm [4] does not compute routes for packets initially. Instead, when a node requests for transfer of data, it checks the current congestion value and then computes the routes accordingly. Our modified form of the Backpressure algorithm [12] does not involve the commodity size during the determination of the route for a particular packet. Since the next-hops are chosen dynamically, depending on the network congestion values, this algorithm can be considered throughput optimal.

The Backpressure algorithm works in two stages:

- Determine the next hops that are to be taken for moving towards the destination
- Selecting the least congested next-hop for the transmission of the arrived packet

2.2 Secret Sharing

The packet is broken into M divisions using a (T, M) threshold secret sharing mechanism such as the Shamir's algorithm [6]. The original information can be recovered from a combination of at least T shares, but no information can be guessed from less than T shares. This approach of secret sharing cannot be effective for both Compromised nodes and DoS attacks.

Secret sharing increases the amount of data that must be transferred from a node to the sink. This in turn affects energy efficiency, bandwidth and also processing capacity of the network. Also no data aggregation technique is used in this approach and every node transmits its data to the sink. Therefore the amount of data transferred is huge and there could be redundant data or even noise in the data that reaches the sink which affects the decision making process.

Data Aggregation[8] or Fusion results in reduced amount of data to be sent over the network, resulting in energy efficiency and filtration of noise along with better understanding of the data to aid the decision making process.

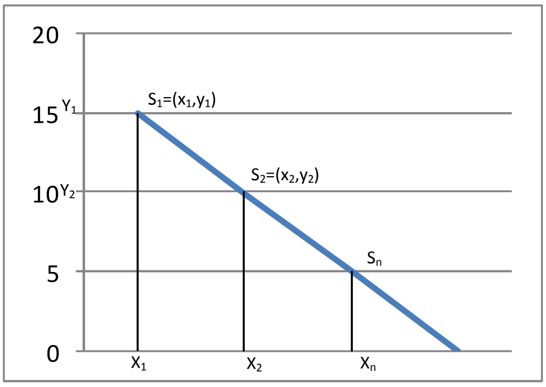

Fig 1: Shamir's Secret Sharing Approach (Degree 1 polynomial and its shares)

2.3 Reactive Routing

The Reactive Routing protocol [11] used here is SENCAST [5]. To find a route in a network, the reactive routing protocol floods the network with a route request and from the returned result, it computes the routes. Since sensor networks can have very low data rate, using a proactive protocol for updating routing tables can be very expensive. Instead, reactive approaches might be more appropriate in such scenarios.

SENCAST is scalable to a very large ad hoc network and adheres to emerging communication scenarios in emergency systems where mobile nodes typically work as a group and are involved in a collaborative manner. SENCAST distributes information efficiently in mobile scenario. It also discovers paths with low overheads by limiting the scope of route discovery packets to a region of potential paths creation. These processes are made possible by using bandwidth and location information. Packet sending is limited by the usage of route reconfigurations.

Hence this algorithm becomes an ideal choice for the transmission of packets in our network.

3. OUR APPROACH

Secret sharing refers to method for distributing a *secret* amongst a group of participants, each of whom is allocated a *share* of the secret. The secret can be reconstructed only when a sufficient number of shares are combined together; individual shares are of no use on their own.

When a sensor node wants to send a packet, it first divides this packet into M shares. These M shares are formed such that a minimum of T shares (where T<M) is required for the reconstruction of the original information.
This ensures us that even if a considerable amount of packets are lost to the black holes, the receiver will be able to retrieve the original information. The maximum number of packets that can be affordably lost are M-T.

The next step is selecting M random nodes from the network. Since this process is carried out in a random format, even the source will not be able to guess beforehand which nodes are to be selected as the intermediaries. The randomness introduced in this phase serves for initial distribution of packets. The packets distributed in this format may not always be moving towards the direction of the sink. So if an adversary listens only in the direction from source to sink, the packets have a probability of taking a different route that is secure and free from black holes.

Each of these M packets are sent to their corresponding random nodes using the Backpressure routing algorithm. The Backpressure routing algorithm takes in the traffic congestion value from the current node for determining the next hop. This way, our packets take the route with minimum congestion, hence this leads to less packet loss and faster transmission. Since traffic during the particular point of time is taken into account, the route for a single node differs from time to time.

The packets that are transmitted to these random nodes are then routed to the sink node by using SENCAST, the Reactive Routing approach. Since this approach uses bandwidth information and the location information, the packets can be transmitted in an efficient manner.

Algorithm

The algorithm for packet transmission using our approach is as follows:

Process followed in the Source Node :

```
1.  Divide the packet that is to be sent into M different
    shares, of which T shares (where T<M) are sufficient
    for obtaining the information

2.  For every packet, perform the following

    2.1   Add the destination node information to the packet header
    2.2   Select a random node
    2.3   Check if the node has already been used
    2.4   If yes goto 2.1
    2.5   Else
    2.5.1     Save the node information in the node list
    2.5.2     Determine the next hop list that is to be taken
              for reaching the random node.
    2.5.3     For each node in the list check for the
              congestion value and select the node that has
              the least congestion value
    2.5.4     Transmit data to that node
```

Process followed in the Receiving Nodes :

```
1.  Check for the packet header whether the particular
    packet is destined for itself.
2.  If yes, check if it has already received T shares.
3.  If yes, aggregate the shares to obtain the
    information.
4.  Else Wait for the T shares to arrive
5.  If the packet is not destined for the current node,
    check for the destination node and transmit the
    packet using SENCAST.
```

Experimental Results

A wireless sensor network is simulated in NS2 (Network Simulator 2) and traffic is configured. Simulations are carried out in varied environments using varying number of nodes and black holes and varying number of packets. Analysis of the network shows that the current system shows an increased immunity towards attacks.

A sample scenario is represented in the Fig 2, in which data from the source node is divided and is passed to the random intermediary nodes (denoted by arrows). These nodes then direct the information to the original sink or receiver node (denoted by dotted lines).

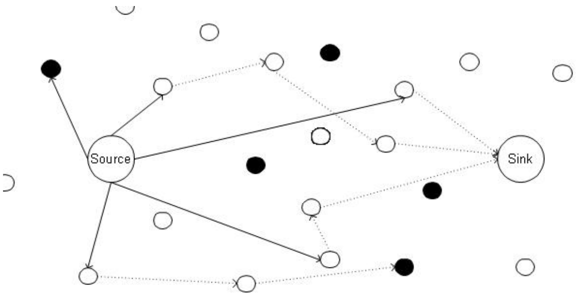

Fig 2: Packet transmission via a network

Fig 2 shows transmission of 5 packets from the source to the sink. Block arrows represent the first phase of transmitting packets through backpressure algorithm and the dotted lines represent the second phase of packet transmission from the intermediary nodes to the sink. The packets have a probability of either directly passing into a black hole or can also move into a black hole on its transmission path. Even if both occurs, a maximum of 3 packets arrive into the destination.

The packets that are sent by the source node have higher probability of circumventing the black holes. Analysis shows that even if a black hole of maximum size is present in the network, the receiver still gets the minimum number of required packets using which rebuilding of information is possible.

4. COMPARISON STUDY

Comparing our proposed technique to the technique proposed in [9], we find that our process is much more secure. According to the older approach, the packets are to be directed towards the source node, for minimizing the delay, but it would become an easy target for the adversary if he/she captures nodes in that direction alone. Since packet dispersion takes place in our approach, the adversary will not be able to predict the direction of packet traversal, hence our approach remains more secure. The use of backpressure algorithm helps in optimal transmission of packets by choosing the congestion free path, unlike the traversals which transfers packets only to the neighbours.

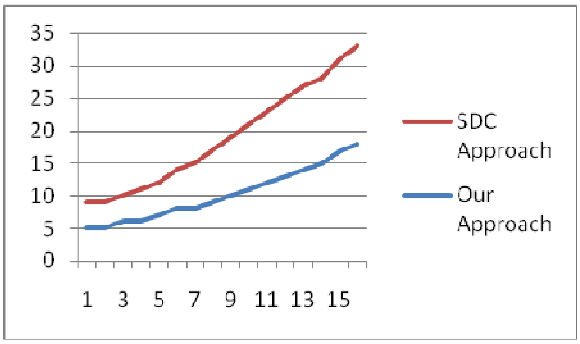

Fig 3: Packets to be sent(X) Vs No of packets after division(Y)

Fig 3 shows the number of packets that are to be sent Vs the number of packets created after division. This shows that our method of division produces lesser amount of packets when compared to [9] and hence helps in avoiding unnecessary network traffic.

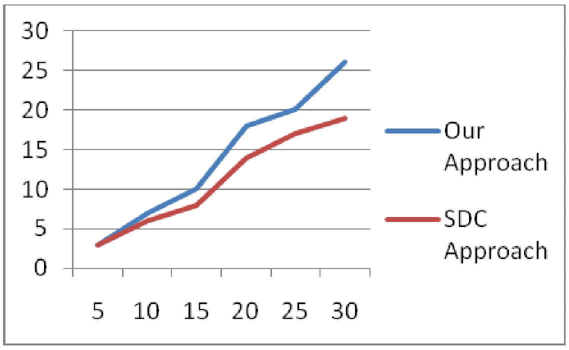

Fig 4: Packets Sent(X) Vs Packets Received(Y)

Fig 4 shows the number of packets that are to be sent Vs the number of packets actually received by the sink. We can say that the number of packets that are received by the sink is more in our approach when compared to other approaches.

Encryption based protocols such as [1], [6] and [7] uses cryptography for solving the security issues. Even though this algorithm is robust and efficient, the encrypted packets are still prone to get lost in the black holes/sink holes. Loosing of necessary packets cannot be avoided. This might in turn lead to inadequate number of packets reaching the destination. This might make the user incapable of obtaining the original information. Since our approach tries to circumvent black holes to the maximum extent, the receiver has a better probability of obtaining the complete information.

5. CONCLUSION

By using the Backpressure algorithm and Reactive Routing methods the packet interception probability can be easily reduced. Though the secret sharing mechanism increases the amount of data transferred from the aggregator node to sink, by optimizing the M value of (T, M) approach to be equal to the number of nodes from which data is aggregated we can overcome this overhead. Thus our approach remains secure when compared to the classic deterministic routing approaches. Denial Of Service (DoS) [9] attacks can be almost made impossible by using out algorithm.

The algorithm can be further optimized by providing the min hop count during the first phase such that the packets are not passed to nodes that are at long distances. The user can also encrypt packets such that even if an adversary obtains a group of packets, they might still not be able to retrieve the information.

6. REFERENCES

[1] Dirk Westhoff, Joao Girao, and Mithun Acharya, “Concealed Data Aggregation for Reverse Multicast Traffic in Sensor Networks: Encryption, Key Distribution, and Routing Adaptation”, IEEE Transactions on Mobile Computing, October 2006, Vol. 5, No.10.

[2] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “A Survey on Sensor Networks,” IEEE Comm. Magazine, August 2002, Vol. 40, No. 8, PP. 102-114.

[3] Blilat Asmae, El Houda Chaoui Nour, Ghazi Mohammed El , Bouayad Anas, “Wireless sensor network: Security challenges”, Network Security and Systems (JNS2)”, April 2012, PP. 68-72.

[4] Michael J. Neely, Rahul Urgaonkar, “Optimal Backpressure Routing for Wireless Networks with Multi-Receiver Diversity, AD HOC NETWORKS (ELSEVIER)”, July 2009, Vol. 7, No.5, PP. 862-881.

[5] P. Appavoo and K. Khedo, “SENCAST: A Scalable Protocol for Unicasting and Multicasting in a Large Ad hoc Emergency Network”, IJCSNS International Journal of Computer Science and Network Security, February 2008, Vol.8, No.2.

[6] D.R. Stinson, “Cryptography, Theory and Practice”, CRC Press, 2006.

[7] G. Ravi, M. Mohamed Surputheen, Dr. R. Srinivasan, “Fast Energy-Efficient Secure Dynamic Address Routing For Scalable WSNs”, IJCSI International Journal of Computer Science Issues, March 2012, Vol. 9, Issue 2, No.1.

[8] Eduardo F. Nakamura, Antonio A. F. Loureiro and Alejandro C. Frery**, “**Information Fusion for Wireless Sensor Networks: Methods, Models, and Classifications”.

[9] Tao Shu, Marwan Krunz, and Sisi Liu, “Secure Data Collection in Wireless Sensor Networks Using Randomized Dispersive Routes”, IEEE transactions on mobile computing, July 2010, Vol. 9, No. 7.

[10] A.D. Wood and J.A. Stankovic, “Denial of Service in Sensor Networks,” Computer, October 2002, Vol. 35, No.10, PP. 54-62.

[11] Harminder S. Bindra, Sunil K. Maakar and A. L. Sangal, “Performance Evaluation of Two Reactive Routing Protocols of MANET using Group Mobility Model”, IJCSI International Journal of Computer Science Issues, May 2010, Vol. 7, Issue 3, No 10.

[12] Scott Moeller, Avinash Sridharan, Bhaskar Krishnamachari, Omprakash Gnawali, “Backpressure Routing Made Practical”.

[13] Modares H, Salleh R, Moravejosharieh A, “Overview of Security Issues in Wireless Sensor Networks”, Third International Conference on Computational Intelligence, Modelling and Simulation (CIMSiM), Sept 2011, PP. 308-311.