IOSR Journal of Engineering
May. 2012, Vol. 2(5) pp: 1200-1206

Security against Selective Forward Attack in Wireless Sensor Network

Arpita Parida[1], Nachiketa Tarasia[2], Tulasi Ambasha Patnaik[3]
[1, 2, 3] *School of Computer Science, KIIT University, Bhubaneswar*

ABSTRACT

Wireless sensor networks (WSNs) are being increasingly deployed for various applications such as object tracking and monitoring, precision agriculture, controlling nuclear reactors, detecting seismic activities, security and surveillance, navigational activities, industrial automation, and so on. In selective forwarding attack, malicious nodes may refuse to forward certain messages and simply drop them, ensuring that they are not propagated any more. In this paper we have proposed a defensive technique. Our approach is divided into mainly three phases: In first phase the node discover a path and its neighbor nodes, in second phase when the event is generated and data is propagated in multipath and is checked whether the data reached is correct or not, and in the final phase if any error is detected then a MONITOR packet is generated and the malicious node is removed.

***Keywords:* – Selective forward attack, Wireless Sensor Network, multi path, route discovery, malicious node**

I. INTRODUCTION

In a span of few years wireless sensor network has significantly increase from many researchers from different fields around the globe. WSNs consist of a large number of small sensor which are low-cost, low-power and multi-functional sensor that are small in size and communication in short distance. The tiny sensor nodes consist of sensing on-board processor for data processing and communication components. Sensor network are networked through wireless links and deployed in large number, provide solutions for monitoring and controlling home, cities and environment [1].

The primary component of the network is the sensor, essential for monitoring real world physical condition such as sound, temperature, humidity, intensity, vibration, pressure, motion, pollutant, etc at different location. WSN has a microcontroller which controls the monitoring, a radio receiver to generate radio waves, different kinds of wireless communication devices and also equipped with energy sources such as battery [2].

There are several properties of wireless sensor networks like self localization, scalability, latency, energy consumption, accuracy, cost, etc.

Basically the WSNs were constructed for Military application like enemy tracking, battle-field surveillances or battle injured estimation, etc. but now a days it is more popular in civil areas too like Habitat monitoring, Environment observation and forecast, Health application and Home and office application [3,4,5]. With the application based in the field of Military application are target of any attack, tracking of new path without human interference, to observe the presence of enemy troop, etc; localization application based on habitat monitoring are target of any wild animal in the forest, target of any forest fire or natural disaster; Health application and home and office can be applied as it provide doctors with medical equipment and personnel for smart hospital, traffic control activities [6].

The major issues for various applications of WSNs are the ability to validate the integrity of the sensor network as well as the retrieved data. Various type of security attack includes (1) the injection of false information in a regular data stream, (2) the alteration of routing path due to malicious node giving false information and (3) the forging of multiple identities by the malicious node. Due to the above reason security plays a major role for the trustworthiness of WSNs. In order to get trusted location information it is necessary to implement location awareness security policies. The organization of more local-dependant services many lead to misuse of data and attack can be performed easily.

In this paper selective forward attack is considered as an attacker in wireless sensor network. In selective forward attack, malicious node will refuse to forward certain message or drop them, making sure that they are not propagated further. A simple form of this type of attack is: when a malicious node behaves as a black hole and refuses to forward the packet it receives. However, such an attacker has a risk that the neighbor node may find other path to route the packet so in order to get detected it forward certain packet and drop certain packet. An adversary interested in suppressing and modifying packet originating from few selected nodes can reliably forward the remaining and limit suspicion of its wrong doings. In case the attacker is explicitly included in a path of a data flow, selective forward attack behaves the most efficient way. Though, it is possible that on overhearing a flow passing through neighbor nodes will be able to implement selective forward attack by jamming or by causing collision on each

forwarded packet of interest. Hence it is proved that when an attacker launches a selective forwarding attack follows the path of least resistance and attempt to include itself on the actual path of data flow [7].
So in this paper we will see how we pass a packet from the event node (where event is generated) to the base station in the presence of selective forward attack and if a selective forward attack is detected then how the node will be avoided for the next phase the packet is sent. Section 2 consists of the related work in security against selective forward attack, Section 3 consist of the proposed work, section 4 consist of simulation result and section 5 contains the conclusion and future work.

II. RELATED WORK

Sophia Kaplantzis et al [8] proposed a simple classification based on intrusion detection scheme that uses the features to detect selective forwarding and black hole based on Support Vector Machines (SVMs) and sliding windows. SVM are a class of machine learning system which has gained popularity due to their ability to handle complex, high nonlinear problem in a consistence, structured manner which simultaneously avoid problems. In this paper one-class SVMs are used in order to detect selective forwarding attack in a sensor network. This intrusion detection is performed in the base station and hence the sensor nodes use no energy to support this added security feature. From this they conclude that the system can detect black hole attacks and selective forwarding attacks with high accuracy without depleting the nodes of their energy.
Bo Yu et al [9] proposed a lightweight security scheme for detecting selective forwarding attacks by using the multipath acknowledgement techniques which increases the detection accuracy but lower the overhead. Unlike common approaches in which detection is implemented in the base station or in a central controller, their scheme lets both the base station and the source nodes have the capability to detect selective forwarding attacks. Thus even when the base station is temporarily inactive by adversaries, attacks can still be detected. Currently their scheme can only discriminate abnormal packet loss from channel error packet loss at a high detection ratio. As long as the malicious nodes, including compromised nodes and outside jammers, cause more packet loss than a normal node does at a certain channel error rate, the attacks are always detectable.
Tao Shu et al [10] proposed a mechanism that generates randomized multi-path routes. Under their design, the route taken by the "shares" of different packets change over time. Several share algorithms are used like PRP (purely random propagation), DRP (direct random propagation), NRRP (non repeated random propagation) and MTRP (multicast tree-assisted random propagation) out of which MTRP share the propagation toward the sink which make it more energy efficient. So even if the routing algorithm becomes known to the adversary, the adversary still cannot pinpoint the routes traversed by each packet. Besides randomness, the generated routes are also highly dispersive and energy efficient, making them quite capable of circumventing black holes. They also formulate an optimization problem to minimize the end-to-end energy consumption under given security constraints.
Satoshi Kurosawa et al [11] proposed a mechanism to detect black hole using a reactive routing protocol known as Ad hoc On–demand Distance Vector (AODV) routing for analysis of the effect of black hole when the destination sequence number has change in a MANET. As black hole is the most important security problem in MANET. It is an attack where the malicious node impersonates a destination node by sending a forged RREP to a source node that initiate route discovery and consequently deprives data traffic from the source node. The algorithm can detect when the destination node has change by its sequence number. So a count of request sent RREQ, count of received messages RREP and average distance between the old destination node and the new destination node which will help in finding where the destination node is forged or not.

III. PROPOSED SYSTEM

In selective forwarding attack, malicious nodes may refuse to forward certain messages and simply drop them, ensuring that they are not propagated any more. A simple form of this attack is: when a malicious node behaves like a black hole and refuses to forward every packet it receives. In order to prevent selective forward attack certain measures are taken in order to detect the malicious node and make sure that the affected node would not be able to participate for the next event tracking process. The whole process has been divided into three steps:

- Route and Neighbor Discovery.
- Transmission of Event Packet.
- Detection of Malicious Node.

3.1 Route and Neighbor Discovery:

Step1: Sink sends the ADVT message to the immediate neighbor nodes.
Step2: After Level 1 is created the nodes in level 1 send a RSSI Signal.
Step3: Then nodes check the neighbor node with highest RSSI signal. If the node is in same level then discards the path else check the neighbor node with highest signal strength which will be selected for path discovery.
Step4: In this way the single path will be generated sink to the source node in a sensor network. Routing discovery is to calculate the number of hops along the shortest path from the source node to the destination node. The sink send out ADVT (Advertisement) Packets and all the neighbor nodes that receive these packets assign themselves as level 1. After the 1st level is created the node existing in first level

send a RSSI (Receive Signal Strength Indicator) to find out their neighboring node. If the result of RSSI falls in the same level then no path from the same level will be considered and if it does not result in same level then node check which of the RSSI signal has highest signal strength. If any signal strength is same then it will select node with lowest node ID. Once we get the node with highest RSSI then the node in level 1 will send ADVT packet to the highest RSSI signal and in this way the path will be generated in a sensor network.

The distance from the sink node to the source node can be assign by the hop count. The hop count determines the distance from the sink to the source node. The hop count is equal to the path length i.e if the hop count from the sink to the source node is 'L' then the path length of the nodes is 'L' hop to the sink. Once the nodes are deployed, the sink broadcast the ADVT packet in order to discover the path from the sink and record the neighbor node, hop count, parent node and the node itself. The hop count is increased by 1 each time when a node receives the ADVT message. While receiving the ADVT message a node considers itself in level 'N+1'. And each time the ADVT message is received by the node it sends a RSSI signal to find out its neighbors. If the neighbors are in the same level then it will discard those paths and select the RSSI with highest signal and make the hop count to increase by 1 and record the parent node along with the hop count. If a smaller hop count ADVT message is received, the node updates its level according to the new hop count. The parameters of the ADVT message are 'Ni', 'Hc' and 'Pi'. Thus the ADVT message is used to model the network into discovering the shortest path and fixed path from each sensor node to the sink node.

3.2 Transmission of Event Packet:

Step 1: Let E be any event which is generated in any node Ni.

Step 2: If the event node does not have a parent node then it will broadcast the event packet to its neighbor node which has parent node.

Step 3: And the parent node will further broadcast the packet to the sink node.

Step 4: Once the event message reaches the sink node then the sink node will check whether the entire event id (EID) received at sink node is same or not.

Step 5: If all the EID are same then No attack is encountered.

Step 6: And an acknowledgement will be send back to the event generated node.

Neighbor discovery is the second phase of the proposed algorithm. In this let us consider let E be any event which is generated at node Ni. Each event which is generated has its unique id denoted by EID, then the event description and time the event is generated. Once the event is generated at any node the node broadcast the event packet as EVENT. After broadcast it check whether the node has a parent node or not, if the node has no parent node then it consider a parameter Hj (hop jump) and count. The hop jump is an integer variable with constant value is taken i.e. when an event is generated the same event is needed to propagated in multipath, in order to establish multipath we should take minimum of two path and maximum of 'n', so we take a fixed value which will be greater than two.

So the event node without parent node broadcast the event detail along with Hj in its own level, once when node Ni receive the packet then the node Ni check whether the node has its parent node. If the node Ni has its parent node then it will decrement the Hj by 1 and sends an acknowledgement to the event node and the process will continue till Hj is equal to 0. Then a condition is checked that if count is greater than and equal to two then the process of propagation packet will take place or else it will again search for another neighbor nodes. But if the event node has its parent node then it will check in its own level the nodes with their respective parent node and wait for acknowledgment packet. When the hop count is equal to 1 i.e. when it reaches the sink node, since we have taken multipath in order to reach sink node, a check is done whether the EID of all the packet are same or not. If the EID is not same then an attack has been occurred and the path will be discarded and would not be considered for the next phase. Final is another integer variable which will store the number of EVENT packet reached with same EID at the sink node. Then sink node sends an acknowledgement to the event generated node. And in this way the EVENT packet helps in forwarding the event detail packet to sink.

3.3 Detection of Malicious Node:

Step 1: If the count compare is unequal then sink will send a ACK packet back to the path from where the event was generated.

Step 2: At the sender end if the node which has send the packet has not receive the ACK.

Step 3: Then the particular node itself generates a MONITOR packet which once sends a message waits for ACK packet.

Step 4: If the ACK is not received then it will mark the particular node as malicious and check for the node in its neighbor without parent.

Step 5: Once the neighbor node is found a new path is considered.

Step 6: if the node does not have neighbor non – parent node then it will send a message to the child node that no further path are available.

The sink node after receiving the event id then will send the acknowledgement to the event generated node. If the source node does not receive the acknowledgement within a particular amount of time then the node which has not received the acknowledgement packet, the particular node

which has not received the acknowledgement will itself generate a packet called MONITOR packet which will have the parameter like Pi and Hc.
Then the MONITOR packet will broadcast to its parent node and wait for acknowledge from the parent node, if the parent node does not reply with the acknowledgement then the malicious node is detected. Once the node is detected the malicious node is removed and kept in mind that it will not be included for the next time for route discovery, and the new path leaving the malicious node will be selected by seeing the neighbor node which does not have parent node and in this way the attack is detected and avoided. If the node does not have a neighbor node then a message will be sent to the child node that no more further path are available. And the MONITOR packet helps in finding the attack in the path and removing it.

3.4 Algorithm:

1. Route and Neighbor Discovery:

Let Ni be any node sending to Nj.
/* on receiving Advertisement packet */
BROADCAST ADV (Ni,Hc)
If (ADV packet receives)
{
If(Hc==0)
{
Hc=Hc+1;
Pj=Ni;
BROADCAST ADV (Ni, Pi, Hc)
}
If (Hc==1)
{
Ni will send RSSI;
If (RSSI of Ni Є Hc==1)
{
Discard the path;
}
Check RSSI with highest strength.
If (any RSSI are equal)
{
Select Ni with smaller value;
}
Hc= Hc+1;
Pj=Ni;
BROADCAST ADV (Ni, Pi, Hc)
}
If ((Ni != sink) && (Hcj> Hci+1))
{
Ni will send RSSI;
If (RSSI of Ni Є Hc==1)
{
Discard the path;
}
Check RSSI with highest strength.
If (any RSSI are equal)
{
Select Ni with smaller value;
}
Hc= Hc+1;
Pj=Ni;
BROADCAST ADV (Ni, Pi, Hc)
}
}

2. Transmission of Event packet:

Let E be any event occurred at node Ni in a network which has a unique EID (event id).
/* after event E has occurred */
BROADCAST EVENT (EID, Ni, Hc, Pi)
If (Ni has no parent)
{
If (Hci == Hcj)
{
Hj = 2;
BROADCAST EVENT (EID, Ni, Hc, Pi)
If (Nj has parent)
{
Hj= Hj-1;
BROADCAST EVENT (EID, Ni, Hc, Pi)
Ni=Pi;
Hc= Hc-1;
}
}
}
Else
{
If (Hci ==Hcj)
{
BROADCAST EVENT (EID, Ni, Hc, Pi)
Ni = Pi;
Hc = Hc +1;
}
}
/* at sink node */
If (Hc == 0)
{
If (Ni ∩ Nj ∩ Nk Є sink)
{
Compare EID if equal;
If (EID are same)
{
Select Ni with greater RE;
}
Send ACK packet to the sender
No Attack detected;
}
}

3. Detection of malicious node:

```
/* At Sender side */
If ( ACK packet not receive)
{
        BROADCAST MONITOR (Pi, Hc)
        Wait for ACK packet
        If (no Ack Receive)
        {
                Node Ni is affected;
                Select new Ni from Neighbor with no parent;
                Establish a new path;
                If( no non-parent neighbor )
                {
                        Send a message to Ni that no Pi exist;
                }
        }
```

IV. SIMULATION RESULT:

Simulation studies of the proposed protocol are carried out to evaluate its performance, and compared its performance with that of Light weight scheme. We describe the simulation model, and the results obtained using Castalia simulator 1.3 [14].

4.1 Simulation Model:

In our simulation, we have varied the number of nodes from 100 to 500, which are randomly deployed in different parts of deployment area with a fixed density. For this simulation, the network parameters, such as transmission range, transmission rate, sensitivity, transmission power etc., are required. The input data is generated randomly in every one second duration at the node where the event occurs and the traffic source is Constant Bit Rate (CBR). We have taken the initial energy of each node to be 29160 joules for 2AA batteries as given in the Castalia simulator. The simulation is run for 2400 seconds therefore each protocol has enough time to discover the route from the sink to the source and produce substantial amount of data traffic.

Number of nodes	100-500
MAC	802.11
Simulation Time	2400 sec
Initial Energy	29160 J
Deployment	Randomly Deployed with fixed density
Traffic Source	CBR
RSSI Range	-100dBm to 0
Transmission bit rate	250kbps
Sensitivity	-90dBm

Table 1. Simulator Parameter

4.2 Performance Metric:

Node Energy Consumption (Ea): The node energy consumption measures the average energy dissipated by the node in order to transmit a data packet from the source to the sink. The same metric is used in to determine the energy efficiency level of WSNs. It is calculated as follows:

$$Ea = \frac{\Sigma_{i=0}^{M}(E_{i,ini} - E_{i,res})}{\Sigma_{i=0}^{M} DataNJ} \quad (Eq\ 4.1)$$

where M is the number of nodes, $e_{i,init}$ and $e_{i,res}$ are respectively the initial and residual energy levels of node i, S is the number of sink nodes and dataNj is the number of data packets received by sink j.

Data Delivery Ratio (R): This metric represents the ratio between the number of data packets that are sent by the source and the number of data packets that are received by the sink.

$$Data\ Delivery\ Ratio = \frac{Successfully\ delivered\ data}{Required\ data} \quad (Eq\ 4.2)$$

This metric indicates both the loss ratio of the routing protocol and the effort required to receive data. In the ideal scenario the ratio should be equal to 1. If the ratio falls significantly below the ideal ratio, then it could be an indication of some faults in the protocol design. However, if the ratio is higher than the ideal ratio, then it is an indication that the sink receives a data packet more than once. It is not desirable because reception of duplicate packets consumes the network's valuable resources. The relative number of duplicates received by the sink is also important because based on that number the sink, can possibly take an appropriate action to reduce the redundancy.

4.3 Simulation Result:

Since Wireless sensor network have very less lifetime so it is necessary that sensor nodes should consume minimum energy in radio communication. From the result in Fig 1 we can find out that the proposed algorithm takes minimum energy as compared to the light weight scheme the proposed algorithm shows lesser energy consumption than the existing system.

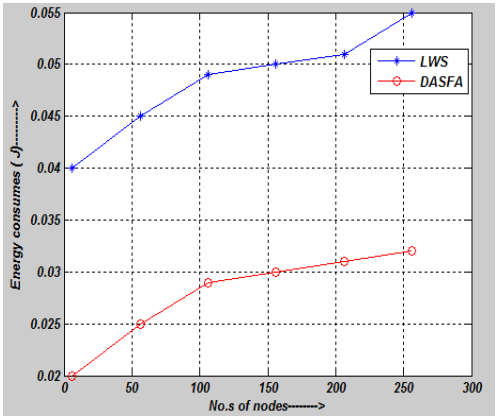

Fig 1. Energy Consumption vs Nos. of nodes

In fig 2 it shows the time spent nodes to transmit a data from the event node to the sink node in presence of compromised node. Here the comparison is made between the Lightweight scheme and the proposed algorithm. The proposed system shows better result than the existing system cause less time is spend.

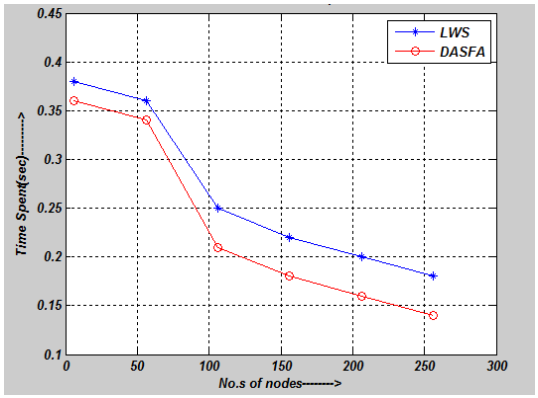

Fig 2. No.s of nodes vs Time spent

In fig 3 the comparison in made between light weight scheme and the proposed algorithm based on delivery ratio and number of nodes in presence of compromised node. This is calculated by the above given formula and the proposed system gives better delivery ratio as compare to the existing system.

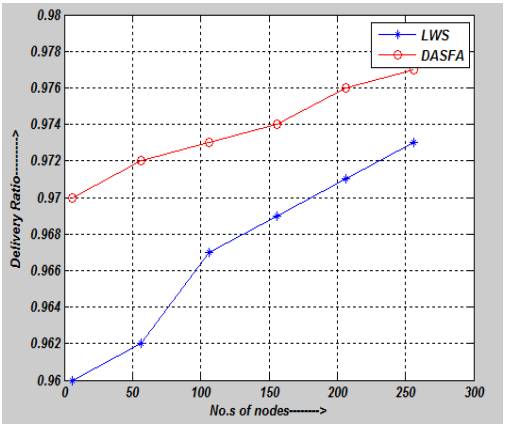

Fig 3. No.s of nodes vs Delivery ratio

In fig 4 the comparison is made of the number of nodes and packet delivery delay between light weight scheme and the proposed algorithm in presence of attacks. The packet delivery delay is less as compared to the existing system.

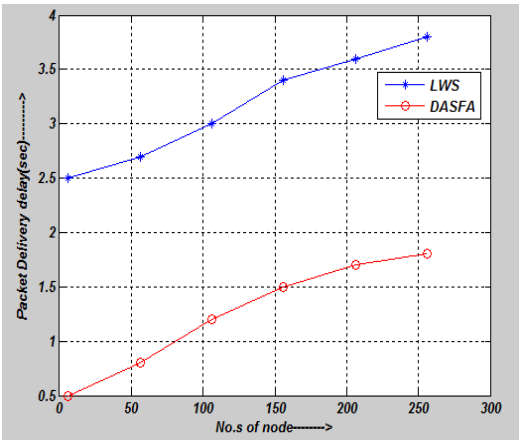

Fig 4. No.s of nodes vs Packet delivery

V. CONCLUSION

Wireless Sensor network has attracted significant research interest because it is vital for many critical applications like traffic monitoring, battle field surveillances, object target finding, soon. Unlike common approaches in which detection is implemented in the base station or in a central controller, our scheme lets both the base station and the source nodes have the capability to detect selective forwarding attacks. Any possibility of the attack can be controlled.

The proposed algorithm creates a single static path after the nodes are deployed in the network and then after the event is occurred how safely and in multipath the packet will reach the sink node. And if any attack is encountered the malicious node is removed and then find a new path so that the connection not to be lost. The simulation results have

also proved that the approach consume less energy, good delivery ratio and can avoid delays. The future work consists of a secret sharing of packet when the event is detected at the event node so that more security can be added to approach this will be strong against wormhole attacks too.

REFERENCES

[1] A.Nilayam Kumar Kamila B.Prasanta Kumar Patra, "A Survey of Routing Protocols for Wireless Sensor Network"

[2] Isaac Amundson and Xenofon D. Koutsoukos, "A Survey on Localization for Mobile Wireless Sensor Networks" Springer-Verlag, Berlin Heidelbeg R. Fuller and X. D. Koutsoukons(Eds.): MELT 2009, pp. 235-254, 2009.

[3] A. Srinivasan and J. Wu, "A Survey on Secure Localization in Wireless Sensor Networks", In Encyclopedia of wireless and mobile communications, B. Furht(Ed.), CRC Press, Taylor and Francis Group, 2007.

[4] A. Cerpa, J. Elson, D. Estrin, L. Girod, M. Hamilton, and J. Zhao, "Habitat monitoring: Application driver for wireless communications technology". In Proceedings of the 2001ACM SIGCOMM Workshop on Data Communications in Latin America and the Caribbean, April 2001, 2001.

[5] Edoardo Biagioni and Kent Bridges. "The application of remote sensor technology to assist the recovery of rare and endangered species." In Special issue on Distributed Sensor Networks for the International Journal of High Performance Computing Applications, Vol. 16, N. 3, August 2002.

[6] Mani B. Srivastava, Richard R. Muntz, and Miodrag Potkonjak. "Smart kindergarten: sensorbased wireless networks for smart developmental problem-solving enviroments." In Mobile Computing and Networking, pages 132.138, 2001.

[7] P. Pandarinath, "Secure Localization with Defense Against Selective Forwarding Attacks in Wireless Sensor Networks" 2011.

[8] Sophia Kaplantzis, Alistair Shilton, Nallasamy Mani, Y. Ahmet Şekercioğlu, "Detecting Selective Forwarding Attacks in Wireless Sensor Networks using Support Vector Machines" intelligent sensors, sensor networks and information ,3rd international conference ,pg 335 – 340,ISSNIP 2007.

[9] Bo Yu and Bin Xiao " Detecting Selective Forwarding Attacks in Wireless Sensor Networks", parallel and distributed processing symposium,20th international, pg 8 pp ,IPDPS 2006.

[10] Tao Shu, Marwan Krunz, and Sisi Liu," Secure Data Collection in Wireless Sensor Networks Using Randomized Dispersive Routes", IEEE Transactions on Mobile Computing, Volume 9 , Issue 7, pg 941-954 , July 2010.

[11] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto, " Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method ", International Journal of Network Security, Vol.5, No.3, PP.338–346, Nov. 2007.

[12] "Castalia a simulator for wireless sensor networks," http://castalia. npc.nicta.com.au/ pdfs/ Castalia User Manual.pdf.