

# Detection of masquerade attacks on Wireless Sensor Networks

Vijay Bhuse<sup>1,2</sup>, Ajay Gupta<sup>1</sup> and Ala Al-Fuqaha<sup>1</sup>

<sup>1</sup> Department of Computer Science, Western Michigan University, Kalamazoo, MI 49008

<sup>2</sup> Institute of Security Technology Studies, Dartmouth College, Hanover, NH 03755

**Abstract**— We propose two lightweight techniques to detect masquerade attacks on wireless sensor networks (WSN). Our solutions take into consideration, important WSN properties like coverage, connectivity, data aggregation and specific communication patterns. The two proposed techniques complement each other when used concurrently. The mutual guarding (MG) technique does not work when nodes are not completely covered by their neighbors or when adversary has shorter transmission range than the sensor nodes. It also does not protect nodes near the boundary. The SRP technique does not have these drawbacks. In this paper, we present our proposed techniques and analyze their performance in terms of successful masquerade detection rate and traffic and computational overhead.

## I. INTRODUCTION

Wireless Sensor Networks (WSN) consist of small devices—called sensor nodes—with RF radio, processor, memory, battery and sensor hardware. One can precisely monitor the environment with widespread deployment of these devices. Sensor nodes are resource-constrained in terms of the RF radio range, processor speed, memory size and power. WSNs follow specific communication patterns as discussed in [5]. Apart from this, sensor nodes are generally stationary. The traffic rate is very low and traffic is periodic as well. There may be long idle periods during which sensor nodes turn off their radio to save energy consumed by idle listening. Recharging or replacing batteries is expensive and may not even be feasible in some situations. Therefore, WSN applications need to be extremely energy-aware.

WSNs are mostly unguarded. Hence capturing a node physically, altering its code and getting private information like cryptographic keys is easily possible for an attacker. Wireless medium is inherently broadcast in nature. This makes them vulnerable to attacks. These attacks can disrupt the operation of WSN and can even defeat the purpose of their deployment. An adversary can launch DoS attacks without much effort (e.g. even without cracking keys used for cryptography-based solutions). Masquerade attacks can be very dangerous because adversaries can launch other attacks and can still hide and project themselves as legitimate nodes. Therefore, masquerade detection mechanisms are necessary. To be practical for real-life WSN deployments techniques for detecting masquerade attacks should be lightweight. Next we discuss WSN topology, trust, and masquerade attack models used in our study.

### A. WSN Model

We assume that  $N$  sensor nodes equipped with isotropic antenna of range  $r$  and sensing radius  $r$  are uniformly distributed in a square area of length  $W$  such that they completely cover the area and remain connected. The base station is placed in one corner of the square area.

Clusterheads aggregate sensor readings from sensors that are in their communication range and forward a single packet towards the base station. Clusterheads are normal sensor nodes and the role of clusterhead is rotated among the nodes. We define *iteration* as the data gathering cycle during which each sensor node sends locally sensed data to the clusterhead and clusterheads forward the aggregated data [3] to the base station. The base station is resource rich whereas sensor nodes are resource-constrained. We assume that the link layer is reliable and that the sensor nodes are stationary.  $PWR$  denote the initial battery power of sensor nodes.  $E_s$  denotes the energy consumed for sending a packet whereas  $E_r$  denotes the energy consumed for receiving a packet.

### B. Trust model

We assume that the base station is physically guarded and cannot be compromised. Every sensor node shares a separate secret key  $K_n$  with the base station. This secret key is used to encrypt the locally detected intrusion information which is sent to the base station. This secret key can be embedded in a sensor node, at design time, while it is programmed. The base station securely informs about the addition of new nodes to their neighbors. Therefore attacker can only masquerade as immediate neighbor. Below we discuss the attack model.

### C. Masquerade Attack model

We consider a setting in which an adversary is added to the network and it assumes the *id* of one of the nodes from  $1$  to  $N$ . There is no deterrent to prevent adversaries from posing as one of the nodes with *id* from  $1$  to  $N$ . Adversaries must follow the MAC protocol being used by nodes in the network.

To the best of our knowledge, we are the first to propose masquerade detection techniques for WSN. In the following sections we present our proposed detection strategies, analyze their performance, draw conclusions and summarize our findings.

## II. PROPOSED DETECTION TECHNIQUES

We propose the two techniques to detect masquerade attacks in WSN. Both techniques compliment each other when used concurrently and enhance the detection probability as shown later. The mutual guarding technique presented in this paper provides a significant extension of the work presented in [2].

### A. MG: Mutual guarding

As stated earlier, nodes are stationary and new nodes are added securely to the network. An attacker can assume the *id* of only the immediate neighbors because receiving a packet from someone that is not a neighbor is an anomaly. Similarly receiving packet with source *id* same as your own *id* is also an anomaly. When two nodes  $s$  and  $d$  are in communication range, the common area (area with stripes as shown in fig. 1) in which the packets sent by both of them can be received is said to be

*mutually guarded* by them. In Fig. 1, when an adversary  $A$  sends a packet to  $d$  by setting source  $id$  to  $s$ ,  $s$  also receives the packet.  $s$  detects the presence of the attacker that masquerades as itself. Thus the adversary cannot masquerade as  $s$  or  $d$  without getting detected when it is located in the common area. Generalizing, when node  $s$  has neighbors around it and if the neighbors' transmission area overlaps with the whole area in which node  $s$  can transmit, then the attacker cannot masquerade as any neighbor to node  $s$ . Receiving a packet sent by  $A$  by changing the source  $id$  to  $s$ , is an anomaly for a node that has never received a packet from  $s$ . A node can thus detect the presence of the attacker that masquerades as  $s$  from these observations.

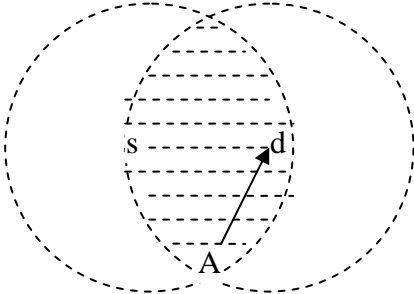


Fig. 1:  $s$  overhears  $A$  masquerading as  $s$ .

The MG method detects presence of attackers that have isotropic antennae with transmission range equal to or greater than that of the sensor nodes. The transmission area of node  $s$  needs to be completely guarded by its neighbors. WSN deployment takes both coverage and connectivity into account and hence MG method works for all the internal nodes (because they are completely guarded by neighbors). Note that if  $A$  has a directional antenna or a shorter range to reach  $d$  but not  $s$  then it will go *undetected* even if it is located in the common area. Our next method called SRP, is more complex but does not have this drawback.

#### B. SRP: Verification of the number of packets sent and received for masquerade detection

As stated earlier, if attacker assumes the  $id$  of a node that is not a neighbor, then it is an anomaly and attacker can be detected easily. Our proposed solution works for MAC protocols that avoid collisions by guaranteeing exclusive access to the RF channel at any given time (e.g. TDMA, 802.11 or CSMA/CA [4] with RTS, CTS, DATA and ACK). Using RF channel random access techniques, adversaries can masquerade the  $id$  of node  $s$  by transmitting data in the time slot allocated to  $s$ . If adversary fails to follow MAC schedule or if collision is detected (for the above collision avoiding MAC protocols) then it is an anomaly. It indicates the presence of an attacker. Our proposed technique can now be described in detail as follows:

Let  $d$  be a node. Let  $s_i$  denote its  $i^{\text{th}}$  neighbor for  $i > 0$ . The following test is performed every  $T$  iterations.  $s_i$  keeps track of distinct number of packets sent ( $S_{sid}$ ) to  $d$  during the time period that lasts for  $T$  iterations. Then  $d$  broadcasts a single packet containing the number of packets it received from its neighbors ( $R_{s1d}, R_{s2d}, R_{s3d}, \dots$ ). If  $R_{sid} > S_{sid}$  then we conclude that there is an adversary (one or more) that masquerades as  $s_i$ . Note that we assume for simplicity of discussion that the link layer is reliable which implies that packet losses due to noise, collisions etc. are

handled reliably and a packet sent is received (albeit may be after retransmits).

Attacker can perform DoS attack on the above solution but it can be detected easily. If adversary broadcasts a packet that  $d$  broadcasts then receivers will receive two such packets (one from adversary and one from  $d$ ) in a time period that lasts for  $T$  iterations. This is an anomaly and it can be guessed that adversary is performing DoS attack on SRP.

### III. ANALYSIS

In this section, we analyze our proposed strategies in terms of success rate of detection, overhead and its effect on the network lifetime.

#### A. MG method

Consider sensor nodes deployed (as shown in Fig. 2) in a square area of length  $W$ . This deployment uses minimum number of nodes to cover the whole area. The deployment shown here is similar to the one presented in [6]. We consider this deployment only for analyzing MG method.

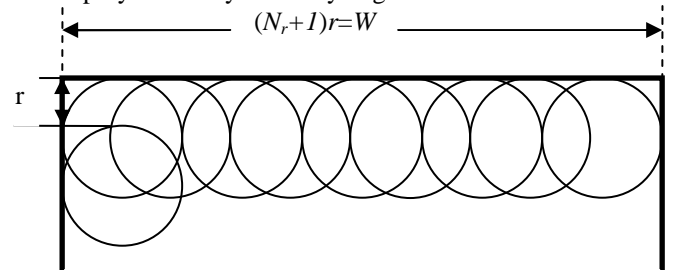


Fig. 2: Optimal deployment for coverage and connectivity; Nodes are located at the center of the circles that are  $r$  apart. The number of nodes in each row be  $N_r$ . Then  $N = N_r^2$  and  $W = (N_r + I)r$ . Therefore  $N_r = \left\lceil \frac{W}{r} \right\rceil - 1$ . Nodes closest to the border are not completely covered. Hence they will not always be able to detect an attacker masquerading as their neighbor.

**Theorem 1:** Attacker has transmission range at least as long as the deployed sensor nodes. Then for the optimal deployment as shown in fig. 2 attacker can assume the  $ids$  of approximately  $8N_r - 16$  nodes if it finds proper place to transmit from and it can perform masquerade attack on approximately  $4N_r - 4$  nodes.

**Proof:** Only the nodes that are closest to the border are not completely covered. In fig. 3, adversary  $A$  can assume the  $ids$  of  $m, n$ , or  $y$ .  $x$  will not be able to detect this masquerade attack because  $m, n$  and  $y$  will not receive the packets sent by  $A$ .

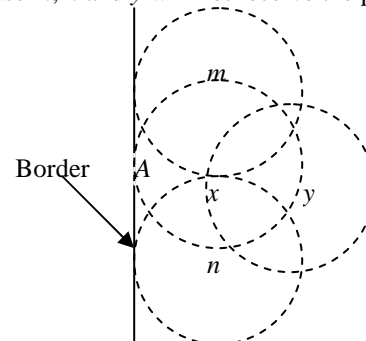


Fig. 3:  $x$  will not detect adversary  $A$  masquerading as  $m, n$ , or  $y$ .

So adversary  $A$  can assume the  $ids$  of nodes that are 1 or 2 hops away from the border if it places itself at an appropriate position while performing the masquerade attack.

The number of nodes that are closest to the border is  $4N_r - 4$  and only these nodes are vulnerable to masquerade attack. Inner nodes are completely covered by their neighbors. The number of nodes that are 2 hops away from the border is  $4(N_r - 2) - 4 = 4N_r - 12$ . Total number of nodes that are not more than 2 hops away from the border is  $8N_r - 16$ . Adversary can assume the  $id$  of any of these nodes while performing masquerade attack. ■

### B. SRP Method

In order to make it difficult for an adversary to guess the transmission time of a node, we can easily assume that nodes transmit packets at a random time during their allotted time slot. Collisions can be detected when packet with stronger signal is received last [7]. With minor modification to the packet structure in fig. 4 (including source address in the tail), collisions in which packet with stronger signal is received first can also be detected [7]. This increases the collision detection rate to a theoretical maximum of nearly 100%. But when two packets arrive at exactly the same time, collision cannot be detected at all [7].

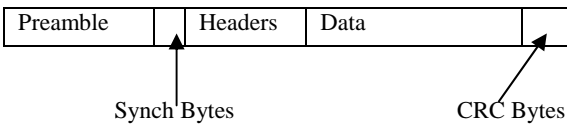


Fig. 4: Packet format (Courtesy [7])

There are two possibilities in this case. (i) Both packets are lost or (ii) One with stronger signal is received.

Adversary can transmit only in the time slot allocated to the node it is trying to masquerade as. If it transmits in the time slot that is not allocated to the node it is masquerading as, then it is an anomaly. Adversary can be easily detected. Let  $p_1$  be the probability with which the packet sent by the adversary overlaps with the packet sent by the node that the adversary is trying to masquerade as. Let  $p_2$  be the probability with which the adversary sends data packet at the same time as  $s$  and collision is detected at the receiver. Let  $p_3$  be the probability with which both packets are lost provided collision cannot be detected. Let  $q$  be the probability with which adversary guesses that the previous packet was lost at the receiver because of interference. It can be noted that it is hard to guess this.

**Theorem 2:** The probability with which the adversary successfully masquerades one packet is  $p_1 \cdot (1-p_2) \cdot (1-p_3) + p_1 \cdot (1-p_2) \cdot p_3 \cdot q \cdot (1-p_1)$ . The probability that the adversary is detected while masquerading  $m$  packets is  $1 - (p_1 \cdot (1-p_2) \cdot (1-p_3) + p_1 \cdot (1-p_2) \cdot p_3 \cdot q \cdot (1-p_1))^m$ .

**Proof:** Adversary successfully masquerades a packet in 2 ways.

In the first case, adversary succeeds in masquerading a packet when (i) the packet sent by the adversary overlaps with the one sent by the original sender, (ii) collision cannot be detected at the receiver and (iii) adversary has sent packet with stronger signal. In this case receiver recovered a packet with stronger signal and it was sent by the adversary. Since collision is not

detected, receiver increments  $R_{sid}$ . Original sender does not know that instead of its packet the one from the adversary with stronger signal is accepted. And it increments  $S_{sid}$ . When  $R_{sid} = S_{sid}$ , SRP is defeated. Therefore probability with which adversary succeeds is  $p_1(1-p_2)(1-p_3)$ .....(1)

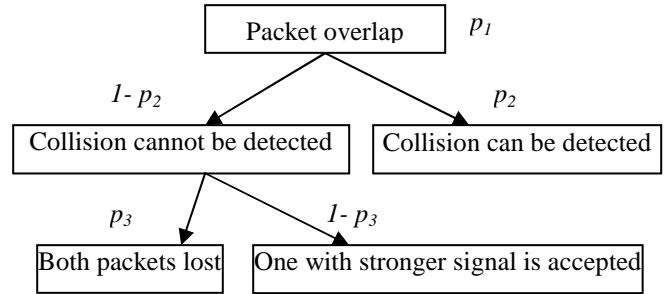


Fig. 5: Probabilities in Lemma 2

In the second case, an adversary successfully masquerades a packet when (i) there is a packet overlap, (ii) collision cannot be detected, (iii) both packets are lost, (iv) adversary guesses that both packets are lost and (v) adversary sends next packet such that it does not overlap with packets from  $s$ .

In this case both (one from the adversary and one from original sender) packets are lost at the receiver and collision could not be detected. Hence original sender does not know that its packet was lost in a collision and the receiver could not detect the collision. Original sender increments  $S_{sid}$ . Adversary sends next packet and receiver increments its  $R_{sid}$  after receiving it. Then  $R_{sid} = S_{sid}$ , and SRP is defeated. The probability with which adversary succeeds is  $p_1(1-p_2) \cdot p_3 \cdot q \cdot (1-p_1)$ .....(2)

Thus, the probability with which adversary succeeds in masquerading a packet is  $P = p_1 \cdot (1-p_2) \cdot (1-p_3) + p_1 \cdot (1-p_2) \cdot p_3 \cdot q \cdot (1-p_1)$ .....from (1) and (2). Probability with which the adversary succeeds in masquerading  $m$  packets is  $P^m$ . Probability with which adversary is detected while masquerading  $m$  packets is  $1 - P^m$  and theorem follows. ■

For overhead analysis, we divide the square area into eccentric circular strips of width  $R=r$  with base station at the center. This helps us count the approximate number of hops for clusterheads located in the strip to reach the base station. Let  $W=cR$  for some constant  $c$ . We call an area “ $k$ -th strip” if all nodes in that area are not farther than  $kR$  and not closer than  $(k-1)R$  for  $k \geq 1$ . So nodes in strip  $k$  are not less than  $k$  hops away from the base station. We compute the area of strip  $k$ ,  $S_k$ , next. From  $S_k$  we compute the approximate number of nodes,  $N_k$ , and the approximate number of cluster heads,  $C_k$  in strip  $k$ . Then we compute the lifetime of the WSN and decrease in lifetime due to periodic SRP is run every  $T$  iterations.

**Lemma 3:** Area of strip  $k$ ,  $S_k$

$$= \frac{\pi(2k-1)R^2}{4} \dots\dots\dots \text{for } 0 < k \leq c$$

$$= \frac{(2k-1)R^2\theta}{2} - 2A_1 - 2A_2 \dots \text{for } k > c$$

$$\text{where } \theta = \frac{\pi}{2} - 2 \cos^{-1} \left( \frac{W}{(k-1)R} \right).$$

$$\alpha = \cos^{-1}\left(\frac{W}{kR}\right) - \cos^{-1}\left(\frac{W}{(k-1)R}\right).$$

$$A_1 = \frac{k^2 R^2 \alpha}{2} - k^2 R^2 \sin\left(\frac{\alpha}{2}\right) \cos\left(\frac{\alpha}{2}\right).$$

$$A_2 = \left[ \frac{-W}{\tan\left(\pi - \sin^{-1}\left(\frac{c}{k}\right)\right)} + \frac{W}{\tan\left(\pi - \sin^{-1}\left(\frac{c}{k-1}\right)\right)} \right] \cdot \frac{R}{2}$$

$$\sin\left(\frac{\pi}{4} + \frac{\theta}{2}\right).$$

$\theta$ ,  $\alpha$ ,  $A_1$  and  $A_2$  are as shown in fig. 6.

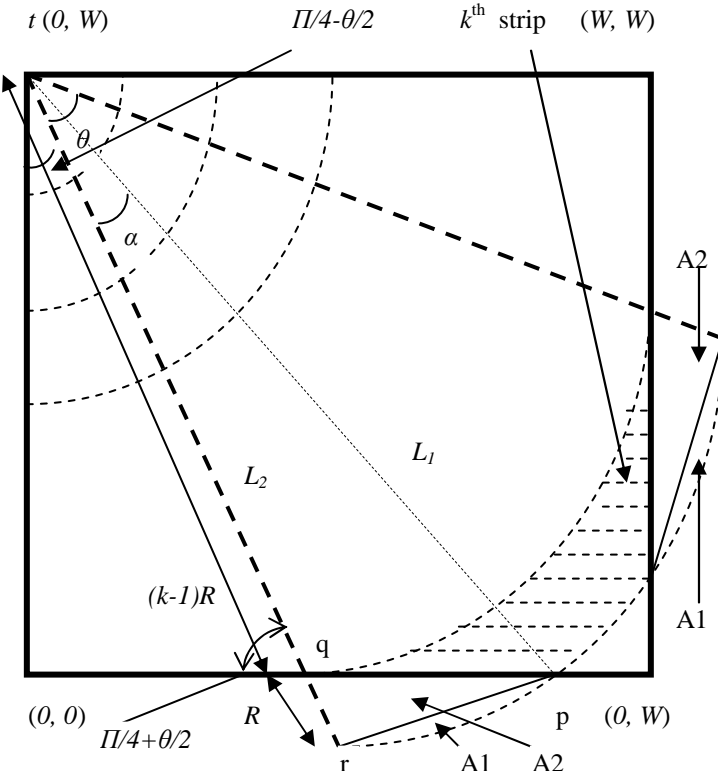


Fig. 6: Area divided into  $c$  strips;  $S_k$  is marked with stripes.

**Proof:** Area of sector with radius  $kR$  and angle  $\theta$  is  $\frac{k^2 R^2 \theta}{2}$ .

Difference between the areas of sector  $k$  and  $(k-1)$  gives us the area of the  $k^{\text{th}}$  strip for  $0 < k \leq c$ . Hence  $S_k = \frac{\pi(2k-1)R^2}{4}$ .....(3)

Next we calculate  $S_k$  strip for  $k > c$ . To calculate  $S_k$  we find the area of the track of width  $R$ , radius  $kR$ , angle  $\theta$  with the center and subtract twice the addition of areas  $A_1$  and  $A_2$ . Fig. 7 shows detailed areas  $A_1$  and  $A_2$  from fig. 6.

From fig. 7(a) it can be shown that  $A_1 = \frac{k^2 R^2 \alpha}{2} - k^2 R^2 \sin\left(\frac{\alpha}{2}\right) \cos\left(\frac{\alpha}{2}\right)$ .....(4)

Details of computing  $A_1$  are not included here because of space limitations.

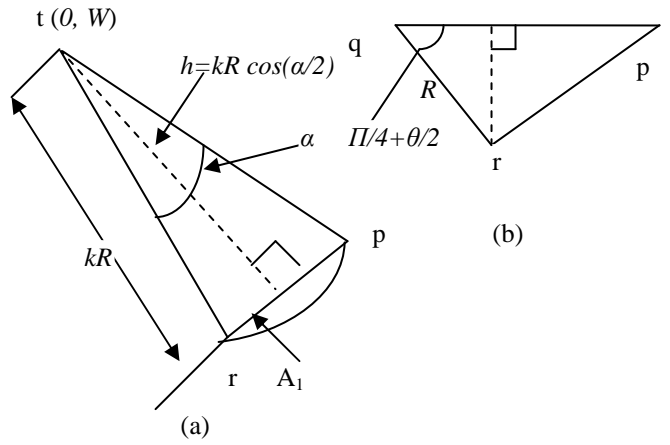


Fig. 7: (a) Area  $A_1$  is shown above; (b)  $A_2$  is triangle  $pqr$ . From fig. 7(b) it can be shown that area of triangle  $pqr$ ,

$$A_2 = \left[ \frac{-W}{\tan\left(\pi - \sin^{-1}\left(\frac{c}{k}\right)\right)} + \frac{W}{\tan\left(\pi - \sin^{-1}\left(\frac{c}{k-1}\right)\right)} \right] \cdot \frac{R}{2}$$

$$\sin\left(\frac{\pi}{4} + \frac{\theta}{2}\right) \dots \dots \dots (5)$$

For  $k > c$ ,  $S_k$

$$= \frac{k^2 R^2 \theta}{2} - \frac{(k-1)^2 R^2 \theta}{2} - 2A_1 - 2A_2.$$

$$= \frac{(2k-1)R^2 \theta}{2} - 2A_1 - 2A_2 \dots \dots \dots (6)$$

By trigonometry, it can be shown (Proof is not included here because of space limitations) that  $\theta = \frac{\pi}{2} - 2 \cos^{-1}\left(\frac{W}{(k-1)R}\right)$

and  $\alpha = \cos^{-1}\left(\frac{W}{kR}\right) - \cos^{-1}\left(\frac{W}{(k-1)R}\right)$ .....(7)

Lemma follows from (3), (4), (5), (6) and (7). ■

Let  $\delta$  be the density of nodes i.e., number of nodes per unit area. Nodes that are in direct communication range from the aggregator form a cluster. Let  $C_i$  be the number of aggregators in strip  $i$ .

**Lemma 4:** The total number of packet transmissions in one iteration i.e., local aggregation by clusterheads and transmission of results to the base station is

$$\sum_{i=1}^K C_i \cdot i + \sum_{i=1}^K C_i (\pi R^2 \delta - 1) \text{ for } C_i = \frac{S_i}{\pi R^2}, 1 \leq i \leq \sqrt{2} c \text{ and } K = \sqrt{2} c.$$

**Proof:** Density  $\delta = \frac{N}{c^2 R^2}$ . Average number of nodes in strip  $k$ ,

$N_k = S_k * \delta$ . Hence the approximate number of clusters in strip  $k$ ,  $C_k = \frac{N_k}{\pi R^2 \delta} = \frac{S_k}{\pi R^2}$  for  $1 \leq k \leq \sqrt{2} c$ . Maximum value of  $k$

(denoted by  $K$ ), is  $\sqrt{2} c$  because length of the diagonal of the

square area is  $\sqrt{2} W$  and  $W=cR$ . Total number of packets sent to all the aggregators by their immediate neighbors is  $\sum_{i=1}^K C_i(\pi R^2 \delta - 1)$ . Total number of packets aggregators send to

the base station is  $\sum_{i=1}^K C_i \cdot i$ . Hence the total number of packet transmissions in one iteration i.e., local aggregation and transmission of results to the base station is  $\sum_{i=1}^K C_i \cdot i + \sum_{i=1}^K C_i(\pi R^2 \delta - 1)$ . ■

Nodes in the first strip do the maximum work by forwarding packets of all the other nodes to the base station. Hence they die first. Therefore network lifetime is the lifetime of the nodes in the first strip. Let  $G_{from} = \sum_{i=1}^K C_i \cdot i$  and

$$G_{to} = \sum_{i=1}^K C_i(\pi R^2 \delta - 1). A_{SRPlife}$$

denotes the network lifetime in number of iterations when SRP is run after  $T$  iterations.  $A_{life}$  denotes original lifetime without SRP. Aggregators in strip 1 receive  $C_1(IIR^2 \delta - 1)$  packets from other nodes in strip 1 and  $\sum_{i=2}^K C_i$  packets from nodes in other strips. They send  $\sum_{i=1}^K C_i$  packets to the base station. The total number of sends

$$performed by nodes in strip 1 is T_1 = C_1(IIR^2 \delta - 1) + \sum_{i=1}^K C_i.$$

$$Whereas total number of receives is R_1 = C_1(IIR^2 \delta - 1) + \sum_{i=2}^K C_i.$$

Therefore approximate lifetime of network in iterations =  $\frac{N_1 \cdot PWR}{T_1 E_s + R_1 E_r}$  where  $N_1$  is the number of nodes in strip 1. Approximate lifetime in iterations of closest nodes,  $A_{life}$

### Theorem 5:

$$A_{SRPlife} = \frac{N_1 \cdot PWR}{T_1 E_s + R_1 E_r + \left( \frac{C_1 E_s + C_1(\pi R^2 \delta - 1) E_r}{T} \right)}$$

when SRP is performed every  $T$  iterations.

**Proof:** When SRP is used, clusterheads in strip 1 transmit  $C_1$  packets to their neighbors ( $R_{sid}$  values) whereas nodes in strip 1 receive  $C_1(IIR^2 \delta - 1)$  packets. The amount of energy consumed by nodes in strip 1 during SRP is  $C_1 E_s + C_1(\pi R^2 \delta - 1) E_r$ . Therefore the overhead (or the energy consumed by SRP) of SRP per iteration is  $\frac{C_1 E_s + C_1(\pi R^2 \delta - 1) E_r}{T}$ . Theorem follows. ■

## IV. RESULTS

To calculate the probability of success of the SRP method, let us assume that packet size is  $b$  bytes and the preamble of the packet be  $b/10$  bytes in size. We say packets overlap whenever a small fraction of the packet overlaps.  $p_1$  is the probability with which the adversary succeeds in guessing the time at which the original node may send the packet. Since WSN traffic is low and intermittent, it is safe to assume that there is quite a bit of idle time during which nodes do not transmit even during their allocated time slots. Hence it is difficult for an adversary to send packet at approximately the time as the original node so that at least some part of packets overlap at the receiver. Therefore we consider values of  $p_1$  from 0 to 0.3 for analysis.

When collision happens, we assume that it cannot be detected even if only a fraction of preambles overlap.  $p_2 = 1 - P(\text{collision cannot be detected}) = 1 - (2 * \text{size of preamble}) / (2b) = 1 - 0.1 = 0.9$ .

It is very hard for an adversary to guess that (i) previous packet collided, (ii) collision could not be detected at receiver and (iii) both packets were lost. But still we give benefit of doubt to adversary and assume that adversary always succeeds in guessing it i.e.  $q=1$ .

For the purpose of analysis we take  $p_2=0.9$  [7]. It can be seen from figs. 8 and 9 that the probability of success is almost 1 when  $p_1$  varies from 0.1 to 0.3,  $p_3$  varies from 0.1 to 1 and  $m$  is 1 or 2. The probability of success increases as  $m$  increase or as  $p_3$  increases. It also increases as  $p_1$  decreases.

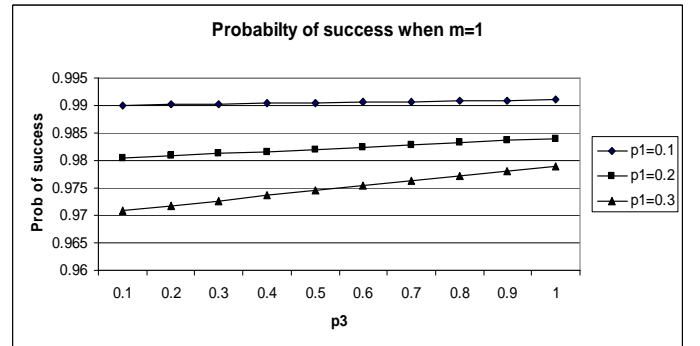


Fig. 8: Probability of success when  $m=1$ .

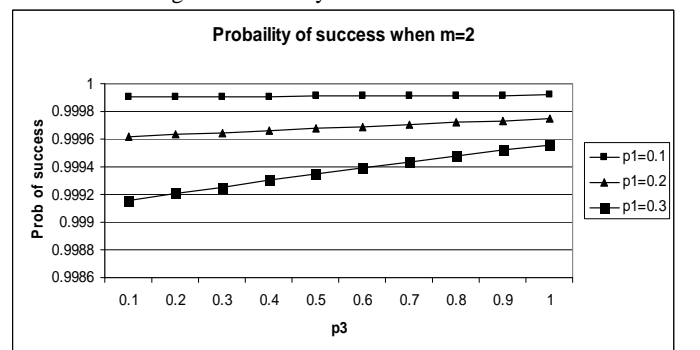


Fig. 9: Probability of success when  $m=2$ .

We use the following parameters [1] to evaluate the overhead of SRP method.

Data rate= 38.4 kbps
Packet size=100 bytes
Max packets transmitted by radio/sec=48

Time for radio to transmit a packet=0.02083 sec
$E_s = 138.3112$ J
$E_r = 54.9912$ J
RC5 encryption/decryption energy per packet= 0.076 mJ.
Initial node energy= $10^8$ J

For  $N=15676$ ,  $r=25$ ,  $W=1000$  we calculate the overhead of the SRP technique. In one iteration data packets from all the nodes reach the base station. The graphs below display % decrease in lifetime when SRP is run after different number of iterations.

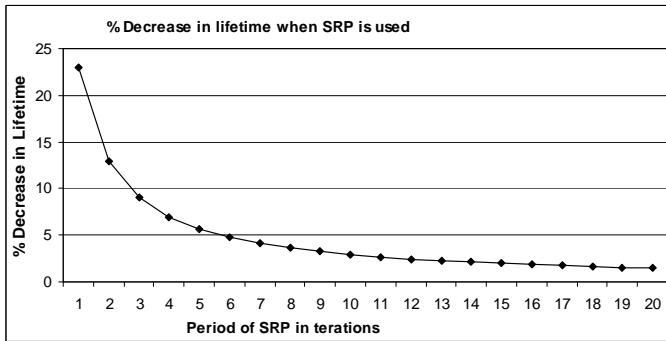
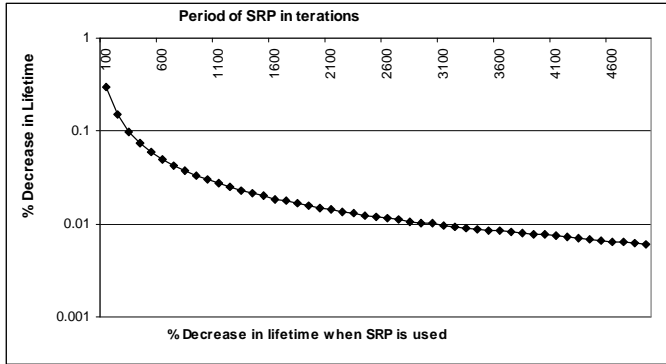


Fig. 10: % decrease in lifetime against number of iterations after which SRP is run.

Network lifetime decreases by 23% when SRP technique is run after every iteration. The overhead is quite small and reduces the network lifetime by only 1% when SRP is run every 30 iterations.

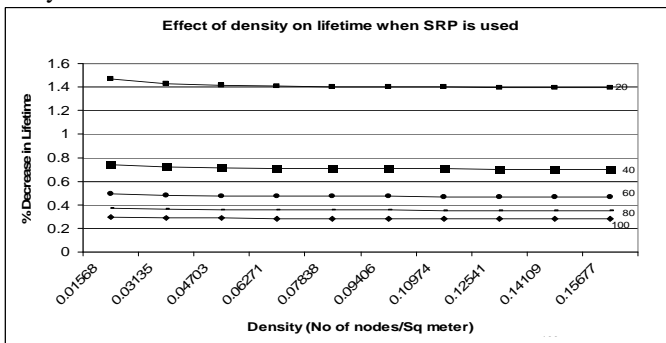


Fig. 11: % Decrease in lifetime for SRP against density of nodes when SRP is performed every 20, 40, 60, 80 and 100 iterations.

Fig. 11 shows the percentage decrease in network lifetime against density when SRP is used after 20, 40, 60, 80 and 100 iterations. It can be seen that increasing density does not increase the network lifetime. This is because all the nodes are busy during the iteration and they are placed uniformly. Of course if some data saving scheme, such as sleep – wake up

schedules, is used then the overall network lifetime will increase by increasing density. But the effect of overhead of SRP on network lifetime will remain the same.

Overhead of MG technique is negligible since it uses passive listening. Data packets are not transmitted. When both techniques can be used at the same time they can cover more scenarios in which attacks can occur. Results of lemma 1 can be included here.

## V. INFORMING BASE STATION ABOUT LOCAL INTRUSION DETECTION

Any node that detects anomaly or intrusion informs the base station securely about it using the shared secret key. This can be done after detecting any type of attack (not just masquerade attacks). This work is part of our general framework for intrusion detection and is not included in this paper.

## VI. CONCLUSIONS

We proposed two lightweight techniques for detecting masquerade attack. Our solutions take into account important WSN characteristics such as coverage, connectivity, aggregation and communication patterns. Our main results can be summarized as follows.

1. Both methods are independent and compliment each other in preventing attacks.
2. MG method fails to protect nodes that are one hop away from the border or when attacker has shorter communication range than sensor nodes. SRP overcomes these drawbacks at a reasonable cost.
3. MG method incurs insignificant overhead as it uses only passive listening. SRP decreases network lifetime by only 1% when it is run after 30 iterations. Overhead of SRP is minimal.
4. The probability of success is very high for SRP.

## REFERENCES

- [1] S. Avancha, "A Holistic Approach to Secure Sensor Networks," Ph. D. thesis, August 2005.
- [2] V. Bhuse, A. Gupta, "Anomaly intrusion detection in Wireless Sensor networks", Journal of High Speed Networks, vol. 15, issue 1, pages 33-51, Jan. 2006.
- [3] B. Krishnamachari, D. Estrin, and S. Wicker, "Impact of Data Aggregation in Wireless Sensor Networks," Proceedings of the 1st International Workshop on Distributed Event-Based Systems, Vienna, Austria, July 2002.
- [4] L. Kleinrock and F. A. Tobagi, "Packet switching in radio channels: Part I", In IEEE Transactions on Communication, volume 23, pages 1400--1416, 1975.
- [5] C. Karlof, D. Wagner, "Secure Routing in Sensor Networks: Attacks and Countermeasures," in *Ad Hoc Networks*, volume 1, issues 2--3 (Special Issue on Sensor Network Applications and Protocols), Elsevier, September 2003, pp. 293-315.
- [6] S. Shakkottai, R. Srikant, N. Shroff, "Unreliable sensor grids: coverage, connectivity and diameter", INFOCOM 2003, Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies, April 2003.
- [7] K. Whitehouse, A. Woo, F. Jiang, J. Polastre, D. Culler, "Exploiting the Capture Effect for Collision Detection and Recovery", The Second IEEE Workshop on Embedded Networked Sensors (EmNetS-II), May 2005.