An Intrusion Detection System for Wireless Sensor Networks

Ilker Onat Ali Miri
School of Information Technology and Engineering
University of Ottawa, Canada
e-mail: ionat@site.uottawa.ca, samiri@site.uottawa.ca

Abstract— **In this paper we introduce a detection based security scheme for wireless sensor networks. Although sensor nodes have low computation and communication capabilities, they have specific properties such as their stable neighborhood information that allows for detection of anomalies in networking and transceiver behaviors of the neighboring nodes. We show that such characteristics can be exploited as key enablers for providing security to large scale sensor networks. In many attacks against sensor networks, the first step for an attacker is to establish itself as a legitimate node within the network. To make a sensor node capable of detecting an intruder a simple dynamic statistical model of the neighboring nodes is built in conjunction with a low-complexity detection algorithm by monitoring received packet power levels and arrival rates.**

Index Terms— **Wireless sensor networks, security, smart sensors, intrusion detection**

I. Introduction

A sensor node is a tiny and simple device with limited computational capability and broadcast power. Wireless sensor networks are generally provisioned to consist of a large number of inexpensive nodes reporting their data to a central, more capable sink node using multihop transmission. In general, it is assumed that sensors will be equipped with non-rechargeable batteries and will be left unattended after deployment. However, current and foreseeable future technology have put severe restraints on energy resources of sensor devices. Because long term operation of nodes with limited battery energy is the main design bottleneck of sensor networks, sensor network protocols have to be designed to operate with minimum resource utilization. Security solutions for sensor networks also have to be designed with the limited computational power, limited memory and limited battery life of sensor nodes in mind.

In general, network security solutions can be grouped into two main categories: *prevention* based techniques and *detection* based techniques. Prevention techniques, such as encryption and authentication, are often the first line of defense against attacks. Detection based techniques aim at identifying and excluding the attacker after prevention based techniques fail. Detection techniques are divided into two major categories: *signature* detection and *anomaly* detection. Signature detection techniques match the known attack profiles with the current changes, whereas anomaly detection uses established normal profiles and detects unusual deviations from this *normal behavior*.

Prevention based techniques are vulnerable to wireless networking challenges. Shared broadcast medium, the possibility of passive listening and resource-limited network elements decrease the effectiveness of prevention mechanisms. The multihop nature of a network also necessitates additional trust requirements among the nodes and increases the vulnerabilities. Although wireless sensor networks have less complex routing requirements when compared to Mobile Ad Hoc Networks (MANETs), securing a sensor network as a whole with prevention based techniques is difficult because of the scalability problems and the computation, communication and storage overhead associated with these methods. There are numerous prevention based solutions for MANETs and wireless sensor networks. There are also a few recently proposed detection based mechanisms for MANETs that we will summarize in the related work section. Neither prevention and nor detection solutions of MANETs can be directly applied to wireless sensor networks. We give more detail about the differences between MANETs and sensor networks affecting the security requirements next.

In this work, we introduce a novel anomaly based intrusion detection method for wireless sensor networks suited to their simple and resource-limited nature. Sensor networks are provisioned to consist of stationary sensor nodes that will provide each sensor with stable neighborhood information. In a distributed fashion, sensor nodes will have the ability to record simple statistics about their neighbors' behavior and detect anomalies in them. The anomalies may present themselves at many different network layers. As long as the implementation is resource-aware, any layer may determine the normals of layer variables and trigger the intrusion alarms for abnormal deviations.

A. Motivation

Although wireless sensor networks belong to the general family of wireless ad hoc networks, they have their own distinctive features. The main differences between the MANETs and sensor networks from the security viewpoint can be summarized under the following titles:

- **Simpler device characteristics:** Sensor nodes are small and inexpensive devices with restricted transmit power (short range) and energy supplies. Due to low computation and communication capabilities authentication and encryption based security solutions are difficult to imple-

0-7803-9182-9/05/$20.00 ©2005 IEEE.

ment in a large scale sensor network. Unlike typical mobile devices, sensor nodes spend a considerable amount of energy not only while sending and receiving data but also in the listening mode [1]. Thus, sensor networks are more vulnerable to resource depletion attacks.

- **Lack of mobility:** In most applications, sensor nodes are stationary. They stay put wherever they are deployed. This decreases routing overhead. Most important, in sensor networks, route request broadcasts of reactive routing protocols and periodic updates of proactive routing protocols either do not occur or occur much less frequently.
- **Large network size:** Sensor networks consist of large numbers of nodes. Security architectures developed for small scale ad hoc networks are infeasible for resource-limited large-scale sensor networks.
- **Stable communication pattern:** In MANETs, nodes are assumed to communicate among themselves (point-to-point). Most MANET applications require transport layer connection mechanisms both for the construction and restoration of flows. However, in sensor networks most of the traffic created as many-to-one sporadic transmissions, as nodes reporting sensor readings to a central, more capable node. In sensor networks, data flow is directional. Each node presumably has a single destination, a next-hop either toward a central node or a clusterhead. This simple forwarding structure is immune to many elaborate routing attacks.

In our detection scheme presented in Section-IV, we exploit the lack of mobility and stable communication pattern.

B. Routing in Sensor Networks

If a sensor network uses an elaborate routing protocol like a MANET, all the attacks against this routing structure will apply to the sensor network as well. A review of such routing attacks and counter measures are given in [2]. The attacks include changed routing information, hello flooding, selective forwarding, sinkholes, wormholes and sybil attacks.

However, since there are no mobility and no point-to-point links, we assume that most large-scale sensor network communications will be in the form of *many-to-one* transmissions as ordinary sensor nodes reporting to single or fixed destinations in a multi-hop fashion with relatively stable paths (similar to rooted trees). There will be no specific communication between the nodes requiring network-wide route request floods. Indeed, in a large scale sensor network, arbitrary point-to-point communication is neither feasible, nor necessary. Instead, a particular sensor node will most likely use only the *next-hop* information to send its own packets and to forward its neighbors' packets for which it is the next-hop. There will also be no mobility and no irregular new node deployments that frequently invalidate this simple forwarding structure.

II. Related Work

A. Prevention Based Techniques

Authentication and encryption based security schemes for sensor networks are adaptations of security algorithms developed for MANETs. These adaptations aim to decrease the computation and communication overhead of these methods which were originally designed for more capable and less resource constrained MANET nodes. An initial overview of security constraints and a variety of approaches for key agreement and key distribution for sensor networks were presented by Carman et al. in [3]. In [4], Perrig et al. introduce a symmetric key cryptography technique adapted to resource limited sensor networks. The architecture in [4] consists of two main building blocks. The first block, SNEP, provides confidentiality, authentication and freshness between source and destination. The second block, μTESLA, provides authentication for broadcasts. In [5], Eschenauer et al. detail a random key distribution scheme for sensor networks. In the key pre-distribution phase, a random key pool is selected from the key space. Each sensor node is randomly assigned a subset of keys from the key pool. The shared key discovery phase occurs after network deployment. A link between two nodes exists only if they are within communication range and they share a key. At the end, if the graph is connected, and if two neighbors do not share a key, a one-hop link between the neighbors can be formed by transferring a path-key over the already existing longer, secure path. Three other random key distribution mechanisms for sensor networks are introduced by Chan et al. [6]. The security analysis of major routing protocols and energy conserving and topology maintenance schemes for sensor networks are explained in Karlof et al. [2] together with major attacks and countermeasures.

Prevention based security schemes are difficult to implement especially over large scale sensor networks. It is not feasible to implement a dynamic public key cryptography scheme and to provide key exchanges with a trusted central authority. On the other hand, symmetric key cryptography can be used to authenticate neighbors. In any case, powerful encryption schemes will not be available because of the computational capacity of the nodes. Thus, security provided to sensor networks with prevention-only techniques is not always sufficient, or practical.

B. Detection Based Techniques

The first Intrusion Detection (ID) based security scheme for MANETs was introduced in [7] along with a general overview of requirements and architectural differences between ID systems for wireline networks and MANETs. In [8], Huang et al. detail an anomaly detection technique that explores the correlations among the features of a MANET node. The work in [9] is a simulation based study of the detection idea introduced in [8]. In [10], some of the MANET routing protocols are used in simulations to detect intrusions where a relatively small number of routing specific features are analyzed using well-known classifiers as anomaly detectors. Authors in [11] present a more coarse-grained intrusion detection technique based on the analysis of packet streams (both data and routing) in an AODV [12] based MANET. Received packets are matched against a number of state-transition attack scenarios describing different attacks.

In [13], the authors propose an intrusion detection system for 802.11 based MANETs using radio frequency fingerprinting. In this work, the idea is that there are unique hardware

characteristics of tranceivers that cannot be forged. The nodes in the network are identified by their signals' transient portion. This enables a basestation to easily identify an intruder using the identity of a legitimate node. The algorithm introduced consists of steps such as calculating the variance of the phase, discrete wavelet transforms, statistical classifiers and Bayesian filter. Although this method is appealing for sensor nodes to identify their neighbors, the very limited computational resources of a sensor node do not allow such a code to be executed efficiently.

Compared to the sensor nodes, dynamic nature of the MANETs necessitates more complex routing protocols. This increases the number of both topology and routing variables. Higher numbers of variables increases the chances of variable interactions which may lead to the detection of even subtle deviations from the normal interactions as shown in [9]. However such complex data mining schemes are beyond the capabilities of the restricted sensor nodes. It is highly unlikely that a sensor node will have the storage and analysis capabilities required by such schemes even with low number of variables. The ID systems designed for MANETs are therefore not suitable for sensor networks.

III. Securing Sensor Networks Using Detection Techniques

In order to prevent powerful intruders disrupting network operations, one has to look at the specific properties of sensor networks. In this context, node cooperation relying on the detection of deviations from expected neighbor behavior may be a feasible methodology. Here, a cooperative solution refers to the attack confirmation and collective action of neighboring nodes against intruders. The following are the key elements required for such a solution:

- Nodes know what to expect from other nodes, particularly from their neighbors. They detect and report anomalies to each other. The essential property of sensor networks that allows for intelligent node decisions is the long term operation of the network with relatively stable neighborhood information for each node.
- Nodes share the unexpected behavior of their neighbors with other nodes. This provides confirmation and common action against the attacker(s).

Next, we illustrate the detection and containment of an intruder using node cooperation. In Figure-1, node *B* is an attacker impersonating a legitimate node. It can be assumed that the legitimate node is destroyed, otherwise a node can easily detect a node using its own id. When the suspicious actions of node *B* are detected by node *A*, it shares this with its relevant neighbors, nodes *F* and *E*. If the overall picture reveals an anomaly, meaning if a node learns that more than a fixed number[1] of other nodes confirm the unusual patterns, it declares the node as an intruder. After hearing the *intruder detected* broadcast, other nodes detecting but not confirming (due to smaller numbers of confirmations) the intruder immediately conclude that *node B* is the intruder. With the overall action of neighbors, the attacker is contained. Detecting nodes may also propagate this information to neighbors that are not yet aware of the intruder.

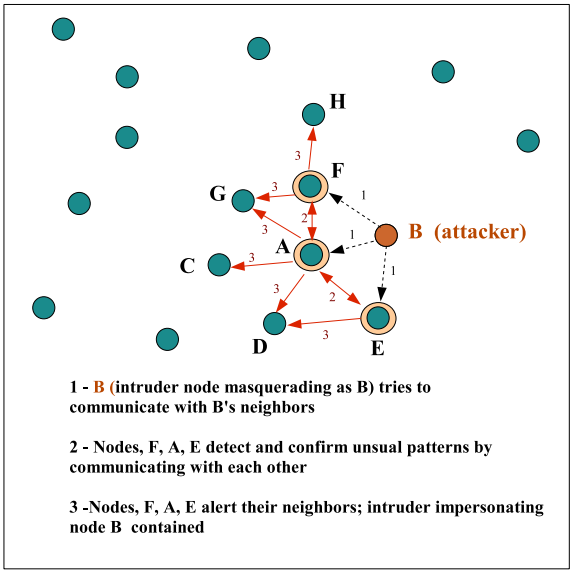

Fig. 1. An intruder containment example

The first step in designing such cooperative containment solutions[2] is the implementation of a node-based statistics gathering and analyzing algorithm. In the remainder of this paper, we address this part of the problem.

IV. Anomaly Detection in Wireless Sensor Networks

A. Attack Models

In this study, we consider the following types of attacks:

- *Node Impersonation*: In order to use or disrupt a sensor network, an intruder has to establish itself as a legitimate node, most likely by spoofing the id of another node. An attacker may then start to deplete the resources of the network or propagate false alarms.
- *Resource Depletion*: This attack can also be seen as the next step of a successful node impersonation attack. Because of the large-scale, multihop and cooperative nature of sensor networks, an intruder can create a high volume of data and control packets that can quickly deplete the batteries of many nodes and disrupt the network.

Nodes keep statistics about their neighbors. The attacks listed above reveal themselves by deviations from the *normal* transceiver and traffic behaviors.

B. Assumptions

We make the following assumptions:

[1] A number selected based on the deployment density.

[2] The detection algorithm implemented does not have to be cooperative. Each detecting node may take independent action without getting confirmation from its neighbors. This may well be enough for containment. However, we believe that low-complexity cooperative solutions may greatly reduce false alarms and increase detection capability.

- The neighbors of a specific node do not change during the course of the analysis. This means three things:
  - Nodes are stationary
  - Transmission power levels do not change
  - No new node is deployed
- Each node can uniquely identify its neighbors (using, for example, a manufacturer assigned id). Nodes do not need to have unique network id's.
- Data and control packet flows are directional and nodes use a tree based forwarding structure as the routing protocol.
- All nodes are peer entities. They use the same hardware with constant transmission power and run the same protocol stack.
- Each node has a clock that does not have to be synchronized with other nodes.

C. Features

The initial step in detection based security systems is the selection of *system features* that will be utilized. Since large scale sensor networks have a rather simple routing structure, stable topology and a low number of control messages, sensor nodes have relatively small numbers of features. We have selected the average receive power (in dBm) and average[3] packet arrival rate (in $packets/unitTime$) as representatives of neighbor activities.

D. Detection Algorithm

Next important step is the selection of a *detection algorithm* which detects intrusion patterns based on the rules. The complexity of a detection algorithm depends on the number and characteristics of system features. A small number of noninteracting features decreases the complexity of the detection algorithm.

We use the following distributed method which is in compliance with the storage and computation capacity of a sensor node. The algorithm has a packet count based *sliding window* approach. At every node, only the last N packets received from each neighbor are used to calculate the statistics for that neighbor and each arriving packet is compared against these values. We call N the *main packet buffer length*. If the packet conforms to the statistics of the neighbor, it is accepted as *normal* and is used for new calculations. The oldest packet's values are removed from the list. We record the *arrival time* and *receive power* of each incoming packet.

To monitor receive powers for anomalies, *min* and *max* values of packet receive power are updated with each *regular* packet reception. An anomalous packet is a packet whose receive power is *below the min* or *above the max* of receive powers currently kept in the main packet buffer of length N. Depending on the sensor network deployment environment and the application, intrusion alarms may be raised with each anomalous packet or after *a predefined number of consecutive packets* show anomalous patterns. In the latter case, anomalous packets have to be kept separate from the regular arrivals until a decision is made. We call the buffer used for this the *intrusion buffer* and represent its length as N_1. This system is shown in Figure-2.

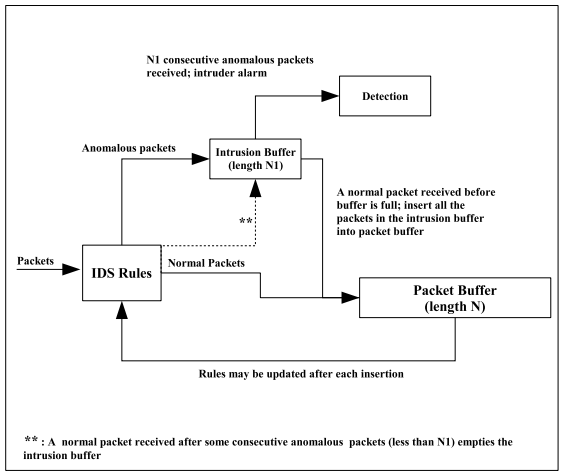

Fig. 2. Receive power anomaly detection

To check packet reception rate anomalies, another packet count is utilized and represented by N_2. We keep two rates: the rate at which the last N_2 packets are received (including the last packet), $rate_{N_2}$ and the rate at which the last N packets are received, $rate_N$. If the ratio of these two rates is above a *comparison rate threshold* called K ($(rate_{N_2}/rate_N) \geq K$) an intrusion alarm is triggered. This method is illustrated in Figure-3.

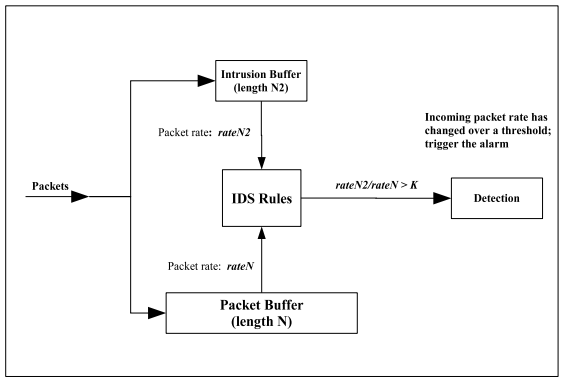

Fig. 3. Packet arrival rate anomaly detection

We also change the value of K to see the effects of changing rules. Our sliding window based approach is suitable for the nodal and operational characteristics of sensor networks. Keeping long term averages with long buffers, using sampling, or using averages updated starting from the beginning of the deployment may lead to false alarms. The slowly decreasing battery power of nodes may raise false alarms due to drops they cause in the transmit powers. The physical changes in the environment may also cause deviations that may seem abrupt when long term statistics are considered. For this reason, in

[3]Here the term *average* is used to refer to the *sample* arrival rate of the packet buffer, not the average rate of the packet generating Poisson process which is represented by λ.

our scheme, we propose keeping an amount of arrival statistics necessary to detect the anomalies but immune to channel fluctuations. The number of packets after which we conclude that the detection has failed is called the *miss threshold* and its length is represented with N_3. If the anomalies go undetected for N packets, they will change the characteristic of the main packet buffer and will never be detected. Therefore, N_3 has to be smaller than N.

Selection of proper N_1, N_2, K and N_3 values depending on security vulnerabilities has crucial influence as these values strongly affect both the probability of detection and the detection time as shown in the next section.

With our proposed power anomaly detection scheme, for a successful attack, the attacker has to keep its relative distance to each node previously hearing from the impersonated node close to the previous distances. If the location of the intruder is significantly different, the possibility of detection due to receive power anomalies increases. To break into the network, the attacker also has to have either the same transceiver circuitry or power control capabilities to perfectly emulate the transceiver of the impersonated node(s). Our arrival rate anomaly detection algorithm forces the intruder to learn the regular packet forwarding patterns of the impersonated node(s).

V. Experimental Results

A. Propagation Model

We assume that the wireless channel does not change during the transmission of a whole packet, however, it is random and independent from packet to packet. We use the log-normal shadowing path loss model [14] to calculate receive power variations at different packet receptions. We assume that the average received power decreases with distance d as $(1/d)^{\beta}$. Random fluctuations around this average are represented by a zero-mean Gaussian random variable called X_{σ} (in dB) with standard deviation σ (also in dB). The general formula for this model is the following:

$$PL(d)[dB] = PL(d_0) + 10\beta log(\frac{d}{d_0}) + X_{\sigma} \qquad (1)$$

In the equation above, $PL(d)$ is the path loss from a distance d. It is calculated using a close-in reference distance d_0. The variable β is called the *path loss exponent* and standard deviation σ is called the *shadowing deviation*. The received signal power, P_r from a distance d is then calculated using

$$P_r(d)[dBm] = P_{tr}[dBm] - PL(d)[dB] \qquad (2)$$

where P_{tr} is the output power of the transmitter. In addition, a packet is received only if its receive power is above a threshold value. In our experiments, in accordance with the results of recent low-power sensor transceiver circuitry and link characteristics research presented in [15] and [16], we used the values listed in Table-I.

B. Intrusion Detection Using Receive Power Anomalies

In this section, we present the results of receive power level anomaly detection capabilities of our algorithm with the simulation parameters given in Table-II.

TABLE I
Shadowing and Transceiver Parameters

Parameters	Values
β	2.5
σ	$5dB$
d_0	$1m$
Transmit power P_{tr}	$5dBm$
Receive power threshold	$-90dBm$

TABLE II
Simulation Parameters-1

Parameters	Values
Initial transmit power (training power) P_{tr}	$5dBm$
d	$25m$
N	100
N_3	25

The Figure-4 represents the probability of false alarm with changing intrusion buffer lengths, N_1 values. In this context, a false alarm means that the algorithm marks the sender as an intruder although the power level variations are only due to the channel variations as modeled by the shadowing model (at constant P_{tr} of $5dBm$).

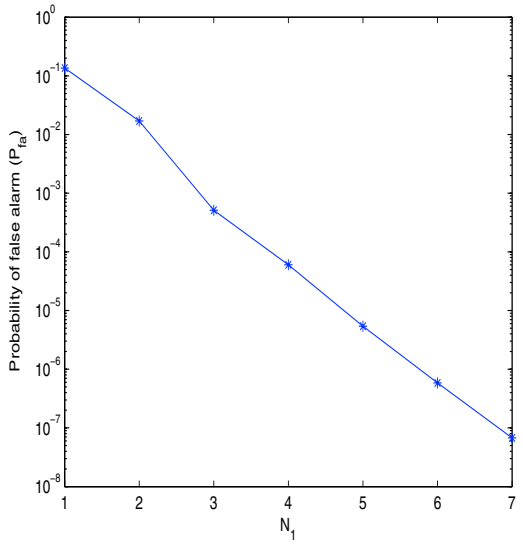

Fig. 4. N_1 vs probability of false alarm

In Figure-5 and Figure-6 we test the performance of the detection algorithm against the sender's actual transmission power changes and for different intrusion buffer lengths (N_1). This experiment requires an initial training period that teaches the detecting node the normal receive power levels of its neighbor. For the first N packets, we keep the transmitter's initial power level of $5dBm$ unchanged. Then the power level of the transmitter is increased and the detection probabilities and detection times are recorded. The number of undetected anomalous transmissions after which we conclude that the detection has failed (N_3) is kept constant at 25.

As expected, when the degree of anomaly increases, it is detected with higher probability and in a shorter period of time. In addition, smaller intrusion buffer lengths (N_1) give

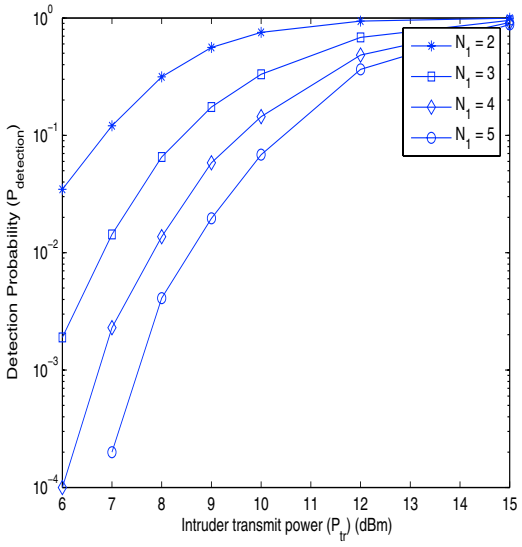

Fig. 5. Intruder power vs detection probability

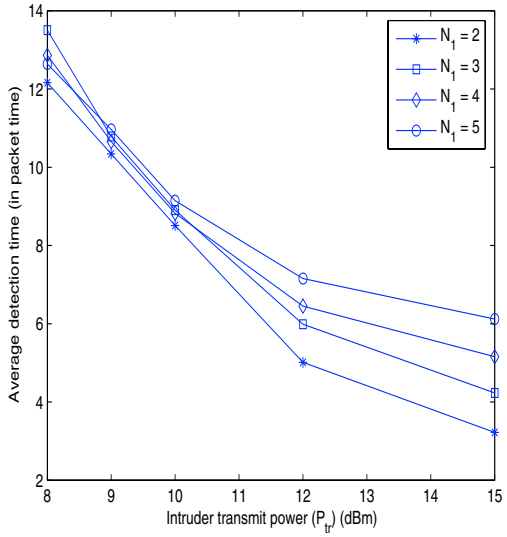

Fig. 6. Intruder power vs detection time

better detection probability and detection delays, however they also increase the false alarm rate. In actual deployments, this trade-off has to be judged according to application security requirements.

C. Intrusion Detection Using Packet Arrival Rate Anomalies

For simplicity, we consider the following traffic model: during a fixed time slot, each node may sense a phenomenon to report with probability p. This means, during that time slot, each node may generate a packet with that probability, independent from other nodes. Therefore, we approximate each node's packet generation as a Poisson process with average rate parameter λ ($packets/unitTime$). We assume a lightly loaded network where there is no queuing delay or other traffic interactions. Thus, the total packets received by each node is a sum of independent Poisson processes which is another Poisson process.

To model the arrival rate anomalies we increase the average packet generation rate of the neighbor to λ_n. The ratio of the two packet reception rates at two buffers $(rate_{N_2}/rate_N)$ is checked against the rate threshold K. If the rate is greater than K, an intrusion alarm is triggered.

Simulation parameters used for arrival rate anomaly detection are given in Table-III. Intrusion detection based on packet arrival rate analysis requires a higher number of previously received packet information, corresponding to higher N, N_2 and N_3 values.

TABLE III
SIMULATION PARAMETERS-2

Parameters	Values
Transmit power P_{tr}	$5dBm$
Initial average Poisson rate (training rate)	$\lambda = 1$
New average Poisson rate	λ_n
d	$25m$
N	1000
N_3	1000

We first check the false alarm probability. Figure-7 represents the probability of a false alarm with changing intrusion buffer lengths (N_2). Here, a false alarm is an alarm raised because of the receive rate variations without an actual Poisson average sending rate change (average rate is constant at $\lambda = 1$ $packet/unitTime$).

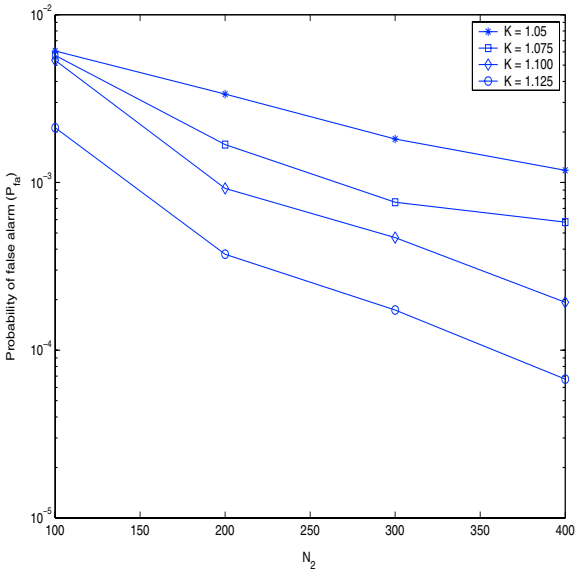

Fig. 7. N_2 vs probability of false alarm

We train the receiver with $N = 1000$ transmissions of average Poisson rate $\lambda = 1$. The intrusion buffer length N_2 is selected as 100 and the detection capability and performance is evaluated as a function of λ_n/λ and with different K values. N_3 is kept constant at 1000. Figure-8 and Figure-9 show detection probability and detection times, respectively.

For the chosen magnitude increases in average Poisson rate, the detection probability and time do not change significantly.

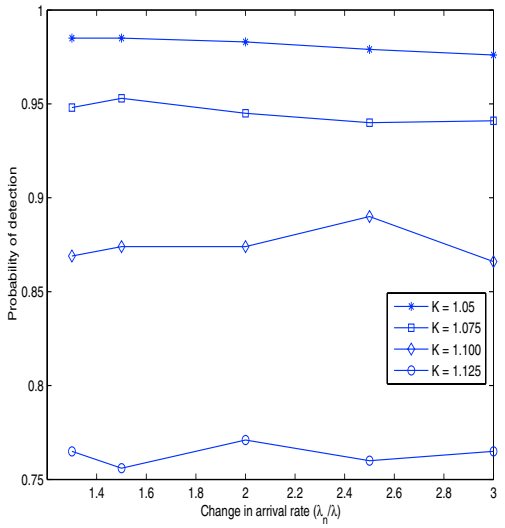

Fig. 8. Arrival rate change (in λ_n/λ) vs detection probability

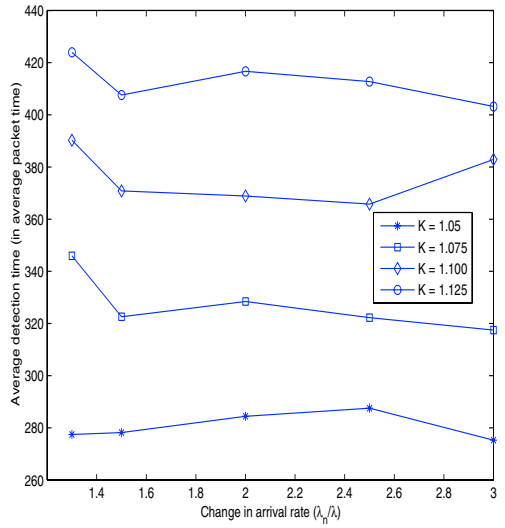

Fig. 9. Arrival rate change (in λ_n/λ) vs detection time

On the other hand, as the rate threshold K decreases, performance of the detection algorithm gets better. However, this also increases the false alarm rate. Again, the selection of K in actual sensor networks is a design decision that relies on traffic and network properties.

The traffic modeling for sensor networks with irregular transmission patterns may be quite complicated. In the packet statistics analysis above, for demonstration purposes, we considered a lightly loaded network where each node creates Poisson traffic. Actual statistics might depend highly on the physical phenomenon monitored. More realistic models will give way to the design of more effective intrusion detection schemes, which we leave for future work.

VI. Conclusion

In this paper, we have introduced a novel anomaly detection based security scheme for large scale sensor networks that exploits their stability in their neighborhood information. If each node can build a simple statistical model of its neighbors' behavior, these statistics can later be used to detect changes in them. We have shown that, by looking at a relatively small number of received packet features, a node can effectively identify an intruder impersonating a legitimate neighbor.

In our implementation, we considered the anomaly detection algorithm executed at each node separately. Low-complexity cooperative algorithms may improve the detection and containment process. Different routing, medium-access and distributed control algorithms will introduce different features. More research is needed to determine better node features addressing specific vulnerabilities and to develop improved detection algorithms with sensor node capabilities in mind.

References

[1] D. Estrin, A. Sayeed, and M. Srivastava, "Wireless sensor networks," *Mobicom Tutorial, availabe at http://nesl.ee.ucla.edu/tutorials/mobicom02*, 2002.

[2] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," in *the Proceedings of the First IEEE International Workshop on Sensor Network Protocols and Applications*, pp. 113–127, May 2003.

[3] D. Carman, P. Kruus, and B. Matt, "Constraints and approaches for distributed sensor network security," Tech. Rep. 00-010, NAI Labs, 2002.

[4] A. Perrig, R. Szewczyk, V. Wen, D. E. Culler, and J. D. Tygar, "SPINS: security protocols for sensor networks," *Mobile Computing and Networking*, pp. 189–199, 2001.

[5] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in *the Proceedings of the 9th ACM conference on Computer and Communications Security*, pp. 41–47, ACM Press, 2002.

[6] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in *the Proceedings of the 2003 IEEE Symposium on Security and Privacy*, IEEE Computer Society, 2003.

[7] Y. Zhang and W. Lee, "Intrusion detection in wireless ad-hoc networks," *Mobile Computing and Networking*, pp. 275–283, 2000.

[8] Y. an Huang, W. Fan, W. Lee, and P. S. Yu, "Cross-feature analysis for detecting ad-hoc routing anomalies," in *the Proceedings of the 23rd International Conference on Distributed Computing Systems*, IEEE Computer Society, 2003.

[9] Y. an Huang and W. Lee, "A cooperative intrusion detection system for ad hoc networks," in *the Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks*, pp. 135–147, ACM Press, 2003.

[10] Y. Zhang, W. Lee, and Y.-A. Huang, "Intrusion detection techniques for mobile wireless networks," *Wireless Networks*, vol. 9, no. 5, pp. 545–556, 2003.

[11] G. Vigna, S. Gwalani, K. Srinivasan, E. M. Belding-Royer, and R. A. Kemmerer, "An intrusion detection tool for AODV-based ad hoc wireless networks," in *the Proceedings of the 20th Annual Computer Security Applications Conference*, pp. 16–27, 2004.

[12] C. E. Perkins and E. M. Royer, "Ad hoc on-demand distance vector routing," in *the 2nd IEEE Workshop on Mobile Computing Systems and Applications*, pp. 90–100, 1999.

[13] J. Hall, M. Barbeau, and E. Kranakis, "Detection of transient in radio frequency fingerprinting using phase characteristics of signals," in *the Proceedings of the 3rd IASTED International Conference on Wireless and Optical Communications (WOC)*, pp. 13–18, 2003.

[14] T. Rappaport, *Wireless Communications: Principles and Practice*. Prentice Hall, 2001.

[15] Y. Chee, J. Rabaey, and A. Niknejad, "A class A/B low power amplifier for wireless sensor networks," in *the Proceedings of the 2004 International Symposium on Circuits and Systems*, vol. 4, pp. 409–412, 2004.

[16] M. Zuniga and B. Krishnamachari, "Analyzing the transitional region in low power wireless links," in *the Proceedings of the IEEE International Conference on Sensor and Ad hoc Communications and Networks (SECON)*, 2004.