SmartDetect: An Efficient WSN Implementation for Intrusion Detection

The SmartDetect WSN Team
Indian Institute of Science, Bangalore and Centre for AI and Robotics (CAIR), Bangalore

***Abstract*—We present the architecture of an intrusion detection application, SmartDetect, that we developed for border and perimeter security over off-the-shelf low cost sensors. The TinyOS implementation of SmartDetect is done on Crossbow's TelosB motes, and home-grown analog Passive InfraRed (PIR) sensor platforms. Our implementation encompasses a suite of algorithms to address specific requirements of the intrusion detection application. Some of the features SmartDetect offers include power-optimal self-organization, reliable message delivery, security, low false alarm event detection, sleep-wake scheduling, energy efficient monitoring and debugging mechanisms. A prototype implementation of SmartDetect has been successfully field tested in an outdoor environment comprising of 25-30 nodes.**

I. Introduction

Wireless sensor networks are used widely in different areas such as agriculture, health-care, industry, defence, hazardous environment, exploration, seismic and structural monitoring, oil and gas pumping, forest fires, etc. We have designed and developed a WSN architecture, SmartDetect, which is robust and feature-rich. SmartDetect can be used in different scenarios to detect human intrusions and reliably communicate such intrusions to the base station in a secure manner. In our work, we primarily focus on border and perimeter security. In this setup the network is expected to work reliably in a harsh outdoor environment with heterogeneous terrain conditions consisting of uneven ground, vegetation, water pools etc. Also, outdoor deployment brings along unpredictable weather conditions, and all these pose many challenges including communication outages, node failures, network voids, and so forth. A low false alarm rate is the critical requirement of the system as false alarms can lead to unnecessary mobilization of security personnel to the perimeter area. SmartDetect addresses all these challenges by incorporating various algorithms in a power-efficient fashion, which ensures long network lifetime. Inclusion of all the important features is possible only with efficient utilization of limited memory available on the sensor device, which SmartDetect accomplishes.

This work is the result of a collaborative effort funded by the Defence Research and Development Organization (DRDO), involving 10 faculty members, and their students and research staff at IISc, and research engineers at CAIR. The complete list of project collaborators is available at http://www.ece.iisc.ernet.in/sensors. All correspondence regarding this submission may be directed to S.V.R. anand (anand@ece.iisc.ernet.in).
978-1-4244-5489-1/10/ $26.00 ©2010 IEEE



Fig. 1. An outdoor setup for demonstrating SmartDetect

SmartDetect is developed over ultra-low power TelosB motes [1] running TinyOS-2.1 [2]. The TelosB mote consists of TI's MSP430 micro-controller with 48KB program memory, 10KB RAM, 1MB Flash, and it operates on two AA batteries. The sensor platform consists of three PIR sensors, connected to TelosB mote, oriented so as to ensure wide angular sensing coverage.

II. SmartDetect Features

The SmartDetect features are implemented as distinct software modules.

Self organization: A power-aware algorithm [3] is used by the motes to come up with a power level such that there exists atleast two nodes which are closer to the base station. This ensures reliable packet delivery to the base station from any point in the network.

Event Detection: A signal processing algorithm based on a 128-bit Haar transform [4] is used to classify the data obtained from the sensors as indicating an intrusion event or otherwise. A distributed fusion algorithm is used to elect a local leader which eventually forwards the event information to the base station.

Routing: A topology-free geographic routing algorithm similar to GRAdient Broadcast (GRAB) [5] is used to route the packet to the base station. The key parameter used in the algorithm is the virtual coordinate of the node from the base station. A GPS can also be used to get the node locations. Only the downstream nodes broadcast the

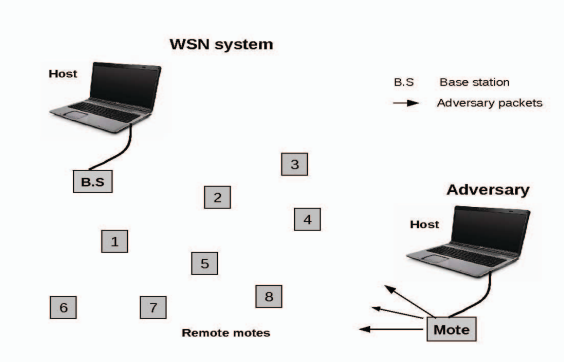


Fig. 2. Demonstration setup

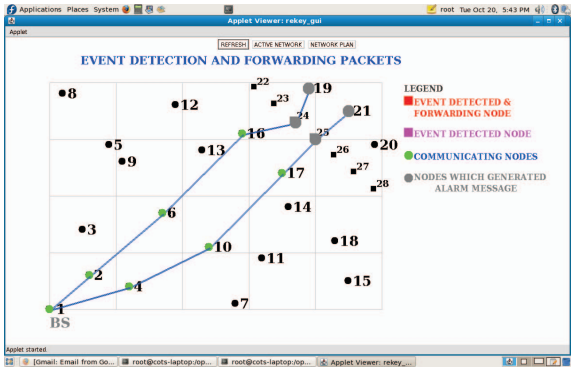


Fig. 3. Example GUI showing the expected result

packet further until it reaches the base station, ensuring loop-free routing.

Network Security: Due to memory constraints, SmartDetect utilizes the components of CCM mode, AES mode, Rjindael algorithm, selectively chosen and modified from Gladman's original C implementation [6]. The code has been appropriately ported to nesC and integrated keeping the functionality intact. This has been used to encrypt and authenticate all the messages in the network using a single shared secret key. In order to improve data confidentiality, a light weight re-keying logic has been implemented by using a low-cost Grindahl hash function. Figure 1 shows the outdoor demonstration setup of WSN intrusion detection application.

Software Contributions

- The application code has been significantly optimized to fit into the low program memory.
- We have created more program memory space for our application by devising a novel two-stage program dissemination process, which was motivated by the large memory footprint taken up by Deluge [2].
- QoS and packet scheduling feature enables prioritization of messages depending on the QoS required by different types of messages.
- Debugging mechanisms built into the code help in in-situ troubleshooting, and monitoring parameters and states of various functional elements. The watch-dog timer makes the system recover from rare but possible pathological conditions.

III. Demonstration Setup and Results

A realistic and impactful demonstration of SmartDetect requires an outdoor environment. Owing to the possible space constraint at the conference site, we plan to demonstrate a scaled-down version with a small number of sensor nodes over a testbed within the alloted stall. We will showcase security and routing features during the demo.

Demo Setup: The demonstration setup is shown in Figure 2, which consists of a base station and several nodes. The adversary is another node in the vicinity of the WSN which tries to disturb the network by injecting packets.

We demonstrate two cases of adversary attacks: i) An adversary who does not possess the secret shared key used by the network injects spurious messages into the network; ii) An adversary having a key used by the network earlier in time, uses that key to inject messages in the network.

Results: The genuine nodes which receive spurious packets fail to decrypt and authenticate the packets, and they raise an alarm which is forwarded to the base station using the geographic routing protocol.

GUI: The result will be displayed on a Java based GUI as shown in Figure 3. The applet shows the network layout of 28 nodes deployed in a randomized grid manner. The gray colored nodes are the ones which have detected spurious packets and forwarded the message. The green colored nodes are intermediate relay nodes. The blue lines indicate the path taken by the packet to reach the base station.

Movie: We will also show a short movie of SmartDetect taken in an outdoor setup which demonstrates power-aware self-organization, intrusion detection which uses distributed signal processing algorithms and geographic routing feature along with the front-end which displays the results at the base station.

References

[1] "http://www.xbow.com/."
[2] "http://www.tinyos.net/."
[3] M. Khan, G. Pandurangan, and V. S. Anil Kumar, "Distributed algorithms for constructing approximate minimum spanning trees in wireless sensor networks," *Parallel and Distributed Systems, IEEE Transactions on*, vol. 20, pp. 124–139, Jan. 2009.
[4] A. Sajana, S. Ramanathan, V. Kumar, S. Krishnan, A. Bharadwaj, S. Jeena, M. Hegde, and S. V. R. Anand, "A low-complexity algorithm for intrusion detection in a pir-based wireless sensor network," in *International Conference Series on Intelligent Sensors, Sensor Networks and Information Processing*, 2009.
[5] F. Ye, G. Zhong, S. Lu, and L. Zhang, "Gradient broadcast: a robust data delivery protocol for large scale sensor networks," *Wirel. Netw.*, vol. 11, no. 3, pp. 285–298, 2005.
[6] B. Gladman, "http://www.gladman.me.uk/."