DSF - A Distributed Security Framework for Heterogeneous Wireless Sensor Networks

Himali Saxena, *Chunyu Ai, Marco Valero, Yingshu Li, and Raheem Beyah

Department of Computer Science Georgia State University
*Department of Computer Science Troy University

Outline

- Introduction
- Related Work
- Network Model
- Problem Definition
- DSF Architecture
- Performance Analysis
- Conclusions and Future Work

Introduction

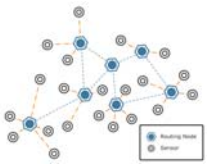
- In the military, WSNs are used for communication, control, intelligence, surveillance, reconnaissance, and targeting systems
- WSNs must be secured since they are given the important role the play
- Current defense techniques only defend against a specific attack (e.g., DoS attack, Sybil Attack)
- The assumption that an attacker will only employ the attack for which the network is prepared to defend is unrealistic
- This approach is analogous to having an antivirus detection engine that contains one signature!

Introduction

- One cannot know what type of attack an adversary will launch *a priori*
- The network must be prepared to defend against all known attacks at any given time
- Naïve approach -> load all the current defense techniques onto the sensor
  - Not feasible because of the memory and storage constraints in sensor nodes
- Having access to all of the defense mechanisms and making them work in concert is a challenging research problem
- We propose combining high-end with low-end sensor nodes to define a general framework for security in sensor networks

Paper in a Nutshell

- WHAT?: To provide a secure framework that protect against all current and future attacks
- WHY?: Current techniques focus on specific attacks
- HOW?: Use a heterogeneous framework where high-end nodes intelligently distribute the most relevant attack defense mechanisms to low-end nodes

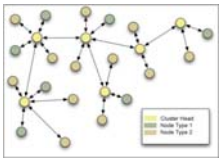


Related Work

- The initial idea of using a heterogeneous framework was proposed in [9] to improve routing
- LIGER [6] provide a hybrid key management scheme for heterogeneous networks. Although some works illustrate the efficacy of using the heterogeneous paradigm to provide security, none provides a comprehensive approach to securing WSNs.
- Some secure protocols (e.g., SNEP and μTESLA[13]) provide data confidentiality and authentication but they do not consider scenarios of malicious activity (e.g., Jamming or DoS).
- Some attacks (e.g., sybil, and wormhole), their detection mechanisms, and countermeasures have been discussed in [3] and [19]. None of the previous approaches combine existing defense mechanisms to provide a general secure framework

Network Model

Clustered Heterogeneous Network



- ***Threat Model and Assumptions:***
  - Gateway nodes are trustworthy and cannot be compromised
  - Attackers possess capabilities similar to legitimate nodes
  - The attacker may change his position to target other clusters
  - If an adversary compromises a node, it can extract all information
  - There may be one attack or several attacks in a single cluster or multiple clusters launched by one or several attackers

Problem Definition

There is a set of attacks A, where:

$$A = \{A_1, A_2, \ldots, A_n\}$$

For any attack A_i there exists a defense scheme D_i. Where D is the set of defense schemes:

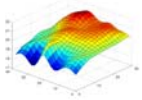
$$D = \{D_1, D_2, \ldots, D_n\}.$$

For each defense scheme D_i the program size is P_i

Since gateway nodes have enough program memory, all defense schemes (*D*), are stored in gateway nodes

Problem Definition

A regular node can only store a subset *S* of *D* since the available program memory $P_r < \Sigma(P_i)$



A *weight* W_{ji} *of* A_i *is assigned for a gateway node* G_j *according to the possibility of the occurrence of the attack* A_i *in* G_j.
The larger the weight, the higher the possibility of attack A_i.

We want to include as many defense schemes as possible in *S*. The defense scheme with higher weight should have priority.

This problem is a 0-1 knapsack problem and our objective is:

$$Maximize \sum_{Di \in S} W_{ji} \quad Subject\ to \sum_{Di \in S} P_i \le P_R, where\ S \subset D$$

DSF Architecture

- ***Routing Protocol:*** Destination Sequenced Distance Vector (DSDV) [24] is used as the routing protocol
- ***Choosing the Defense Mechanism Subset:***

Attack	Program size
Sinkhole	4KB[[5]]
Hello Flood	1KB[[1]]
Jamming	5KB[approx]
Wormhole	5KB[approx]
DoS	5KB[approx]
Selective Forwarding	1KB[approx]
Sybil	4KB[approx]

We divide attacks in different categories based on our opinion of their security level. The *weight is assigned to indicate how dangerous it is to the network* (this can be easily changed)

Category 1	Category 2	Category 3
Selective forwarding	Sybil	Wormhole
Hello flood	Sinkhole	Jamming
-	-	DoS

DSF Architecture

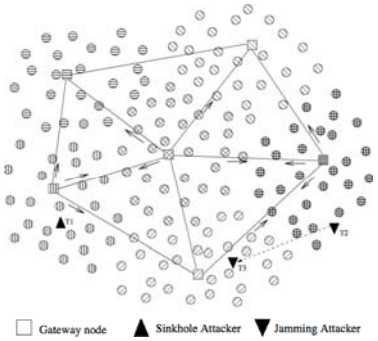
How it works:

1. Gateway detects attack A_i and sends a warning W_k to all gateway nodes including A_i, sender ID G_s, and weight of this warning WW_k
2. Once a gateway G_j receives a warning W_k, it updates the received warning list L_j
3. For each attack A_i in L_j, we calculate the weight W_{ji}

$$W_{ji} = \sum_{\forall W_k \in L_j \text{ and attack is } A_i} \frac{WW_k}{D(G_s, G_j) * (T_c - T_k)}$$

4. After calculating weights, a gateway solve the 0-1 knapsack problem to obtain *S*. If *S* is not in the cluster, deploy a new set of images *S* using Deluge.

The Security Framework



Performance Analysis

Network Settings

Parameter	Setting
No. of regular nodes	2000
No. of gateway nodes	10
Network size	1000 m *1000 m
Transmission range of regular node	50 m
Transmission range of gateway node	500 m
Initial energy of regular node	1 J
Energy cost for sending a message by regular node	10 uJ
Energy cost for receiving a message by regular node	1 uJ

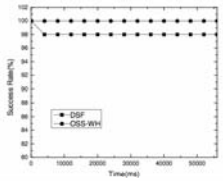
Two metrics are used to evaluate the performance of DSF:

1) **Success Rate: Percentage of nodes alive after the attacks**
2) **Energy Consumption: Average percentage of residual energy for all currently alive regular nodes**

Performance Analysis

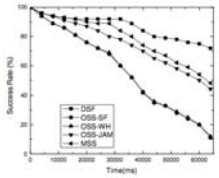
➢ **Comparison between DSF and OSS-WH in case of only one attack:**

200 wormhole attacks are injected, and initially the DSF does not install the wormhole defense scheme.



➢ **Success Rate: Static Attackers.**

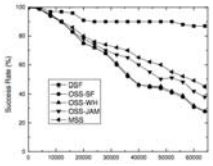
200 attacks randomly which alternate between the 7 attacks.



Performance Analysis

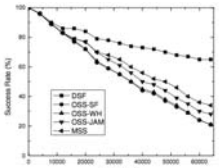
➢ **Success Rate: Mobile Attackers**

10 attackers are mobile in the network with the speed of 10 m/s injecting various attacks randomly.

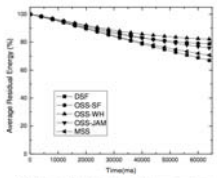


➢ **Success Rate: Static Attackers and Mobile Attackers**

Both static and mobile attackers are loosely scattered in the network.



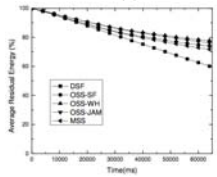
Performance Analysis



The following three charts shows average residual energy percentages for the same three previous scenarios

➢ **Energy Consumption: Static Attackers**

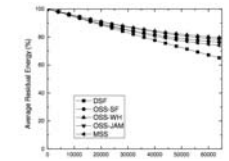
MSS scheme has 10% more average residual energy than the DSF.



➢ **Energy Consumption: Mobile Attackers**

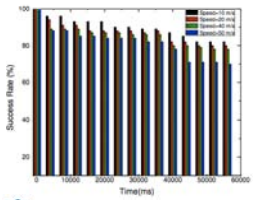
OSS-SF, OSS- WH, and OSS-JAM schemes have approximately 20% more average residual energy than the DSF

Performance Analysis



➢ **Energy Consumption: Static Attackers and Mobile Attackers**

The DSF consumes more energy than OSS and MSS. **More energy used to keep more nodes alive by deploying defense mechanisms and warnings.**



➢ **Effect of Speed of Mobile Attackers**

The attacker with maximum speed is able to comprise the most nodes

Conclusions

- **We presented a distributed security framework (DSF) for heterogeneous wireless sensor networks**
- **We dynamically use the available memory space of regular nodes to store a subset of defense schemes to provide security against multiple attacks**
- **Our warning scheme can enable the regular nodes to install the defense schemes in advance of potential forthcoming attacks.**
- **DSF performs well in the presence of static as well as mobile attackers, each with multiple types of attacks.**

Future Work

- We plan to improve the success rate by determining the optimal subset of installed defense mechanisms for individual sensor nodes instead of every cluster
- We plan to address the case where a gateway node generates false positives and false negatives
- We plan to implement the framework on real sensor motes and verify its attack resistance in the presence of various attacks
- We plan to consider thrashing attacks of the DFS where the attackers deliberately alternate attacks to drain the energy of the system

Questions?

www.cs.gsu.edu/cap
rbeyah@cs.gsu.edu