A SECURE OPTIMUM DISTRIBUTED DETECTION SCHEME IN UNDER-ATTACK WIRELESS SENSOR NETWORKS

1. ABSTRACT

We address the problem of centralized detection of a binary event in the presence of _ fraction falsifiable sensor nodes (SNs) (i.e., controlled by an attacker) for a bandwidth constrained under attack spatially uncorrelated distributed wireless sensor network (WSN). The SNs send their one-bit test statistics over orthogonal channels to the fusion center (FC), which linearly combines them to reach to a final decision. Adopting the modified deflection coefficient as an alternative function to be optimized, we first derive in a closed-form the optimal weights combining. But as these optimal weights require prior knowledge that cannot be attained in practice, this optimal weighted linear FC rule is not implementable. We also derive in a closed-form the expressions for the attacker "flipping probability" (defined in paper) and the minimum fraction of compromised SNs that makes the FC incapable of detecting. Next, based on the insights gained from these expressions, we propose a novel and non-complex reliability-based strategy to identify the compromised SNs and then adapt the weights combining proportional to their assigned reliability metric. In this way, the FC identifies the compromised SNs and decreases their weights in order to reduce their contributions towards its final decision. Finally, simulation results illustrate that the proposed strategy significantly outperforms (in terms of FC 'sd election capability) the existing compromised SNs identification and mitigation schemes.

2. SCOPE OF THE PROJECT

The framework of distributed detection under attack free WSNs have been extensively studied in, to name but just a few. While references consider distributed detection by assuming unlimited bandwidth/resources in WSNs, the authors of relax this assumption by considering distributed detection over bandwidth-constrained/energy constrained WSNs. But these approaches are vulnerable to security attacks as some of the SNs reporting to the FC maybe compromised. As a result, the FC is not robust against such attacks and its detection performance will be degraded.

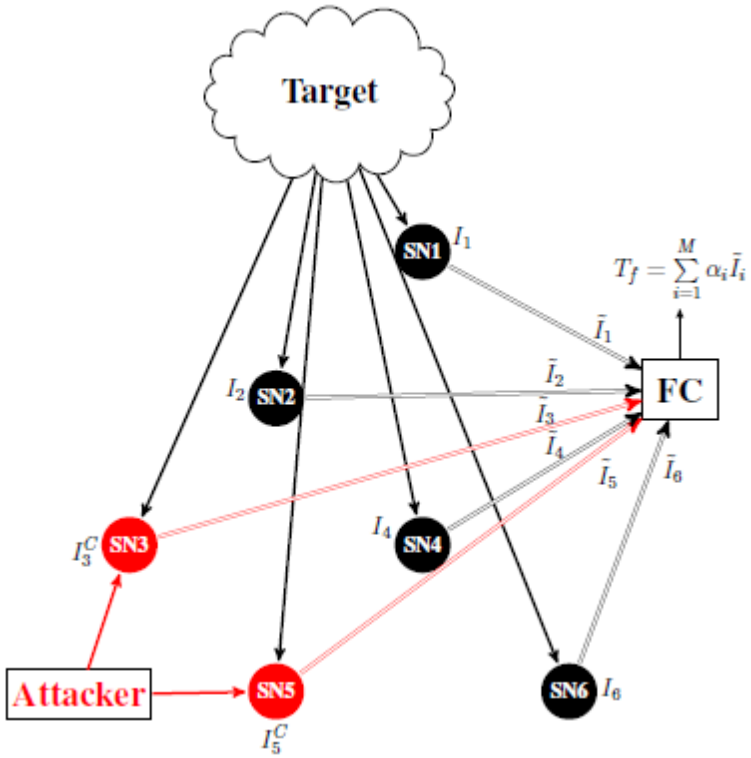
3. PROBLEM STATEMENT

Now, security vulnerabilities can be exploited by different types of attacks that can be launched in a WSN, for example, jamming, spoofing, wiretap disruption attacks, etc. Apart from these well-known traditional security threats, several recent studies consider the sensor node data falsification (SNDF)attack (known as a Byzantine attack. The Byzantine attack was first proposed by and later widely used in the context of distributed detection (and see references therein). In this work, we also consider the SNDF attack in which the compromised SNs send wrong local decision reports to the FC either to degrade the FC detection performance or to achieve their selfish greedy objectives.

4. COMPARISON OF PROPOSED AND EXISTING SYSTEM

EXISTING SYSTEM	PROPOSED SYSTEM
➢ Existing schemes use reliability-based metrics to possibly identify the compromised SNs and then totally exclude them from contributing to the FC process and decision. ➢ However, identifying and then excluding them from the detection process is not the optimum solution. ➢ Whereas the existing schemes totally exclude the compromised SNs (i.e., a zero weight is assigned) from the fusion process.	➢ Different from the existing approaches, here we propose to update the weight combining of each SN based on the correctness of information reported to the FC. ➢ We also proposed a new reliability metric and based on this, a reliability-based scheme was presented to identify the compromised SNs in the network and to control their contributionstowards the FC's final decision. ➢ This new approach decreases the weights of the compromised SNs proportional to the reputation metric
DRAWBACK: The existing FC rules and the compromised SNs identification schemes.	***ADVANTAGE:*** The proposed approach significantly outperforms, in terms of detection performance improvement

5. PROPOSED SYSTEM



5.2 Proposed System Technique Explanation

Our main contributions are as follows:

(i) First, we develop an efficient FC linear weight combing framework for an under□attack WSN. To further reduce the optimization complexity and to get an insight into the problem, we adopt the modified deflection coefficient (MDC) as an alternative function to be optimized. Based on this (i.e., the MDC), we provide an optimization problem to be solved from both the FC's and the attacker's perspective. From the FC's perspective, we derive analytically (in a closed form) the optimal weight combiner for each SN. We show that these weights are a function of the local SNs probability of false alarm and probability of detection

metrics as well as the SNs local test statistics “flipping probability” (to be defined later).Unfortunately, for the compromised SNs this a priori knowledge cannot be obtained in practice (we propose a solution to this. Then (from the attacker’s perspective), we derive analytically (for a fixed number of compromised SNs) the optimum attacker local test statistics flipping probability

and the minimum fraction of the compromised SNs that makes the FC incapable of detecting.

(ii) Next, based on this framework (i.e., FC linear weight combing strategy), we also propose a new non-complex and efficient (based on a reliability metric) FC detection scheme to identify the compromised SNs.

6. SOFTWARE REQUIREMENT

- Linux Ubuntu 14.04
- NS2
- OTCL
- NAM
- X-Graph
- Trace Graph
- C++
- AWK