Enhanced intrusion detection and identification in wireless sensor networks

William S. Hortos

Model-based 'opinions' of data and their aggregates replace the probabilistic weights in a neural algorithm to improve accuracy and response times.

Ad hoc wireless sensor networks (WSNs) offer area surveillance that affords rapid, flexible deployment in arbitrary threat environments (such as the battlefield scenario shown in Figure 1). Without infrastructure support, sensor nodes communicate with each other only when they are within wireless-transmission range. The nodes are typically unattended and severely resource restricted, with limited processing, memory, and power capacities. They work cooperatively to process and fuse sensor data relevant to the mission’s information needs. Each sensor at a node observes physical phenomena within its sensing range. Node processing quantizes and fuses these observations to produce aggregate information. This occurs along an intermediate sequence of wirelessly linked nodes that terminates at the sink (destination) node. The wireless medium can be easily eavesdropped, and links forming network paths and their constituent nodes can be compromised by intrusion attacks from malicious agents operating either outside the network or internally at the nodes. Node compromise can introduce uncertainties into the aggregate information. A compromised node may completely reveal its operations to the adversary, thus rendering purely cryptographic approaches vulnerable. Finding methods to secure data fusion against attacks by compromised nodes and quantify uncertainties that may exist in the fused data becomes critical in mitigating the effects of such intrusion attacks.

In previous approaches we selected parameters from network-protocol layers to detect and identify certain intrusion attacks. Our algorithms (both supervised and unsupervised) improved the residual performance of intrusion-prevention measures provided by dynamic key-management schemes and trust models implemented among nodes. Unsupervised algorithms are not trained on the signature of known attack traffic but instead learn that of normal network traffic. However, the detection and identification accuracy for the unsupervised approach is significantly lower than that for the supervised learning techniques applied to the same intrusion-attack scenarios.

In addition, traditional detection approaches (based on pattern matching and static cryptographic signatures) are limited in their response to the continuous evolution of attacks against WSNs, since they need up-to-date, comprehensive knowledge bases. Data-mining techniques have been applied successfully in host-based intrusion-detection approaches, but extending these techniques to raw network data is complicated by the enormous input-data volume that could potentially exhaust the limited processing resources. These limitations stimulated development of a new unsupervised approach to intrusion detection and identification in which the set of discrimination parameters is augmented with the security attributes and quantified trustworthiness (reputation) levels established during data exchanges among nodes.

Figure 1. Wireless-sensor deployment in a typical battlefield scenario.
Previously published research has introduced the concept of the ‘reputation’ of a single sensor node. Reputation is evaluated using an information-theoretic concept, the Kullback-Leibler distance, which can be added to the set of security features. During data fusion, an ‘opinion’ (a metric of the degree of belief) is generated to represent the uncertainty in the aggregated result. As the fused information is disseminated along network routes to the sink node(s), its corresponding opinion is propagated and regulated by Jøsang’s belief model. This model allows effective quantification of the uncertainty within the sensor data and their aggregation throughout the network. In principle, the concept of opinion can be used to interpret the degree of trust about the fused result. By applying subjective logic to the opinion to manage trust propagation, the uncertainty inherent in fused results can be precisely quantified for use in decision making by security algorithms.

However, key assumptions must be made regarding the reputation and opinion of data to evaluate the uncertainty of a fused result that preclude their application in security algorithms for dynamic WSNs. The notion of reputation assumes that the system of data sources is stationary. Moreover, a computational algebra is usually introduced to generate the sequence of propagated opinion (reputation) values along network routes that leads to increasingly complex calculations by limited processors at successive nodes (and to excessive overhead in the data-fusion process).

Instead, we modify these concepts to allow their application to WSNs in arbitrary threat environments. First, we incorporate the sequence of sensed-data acquisition times with the temporal correlation of data from like-kind sensors to evaluate the opinion of fused results. Second, we reduce the computational complexity of opinion evaluation for propagated, fused results. The computation is decomposed into a sequence of processing steps that are performed simultaneously with data fusion at successive nodes. Each step computes the interim opinion value at a processing node along a route based on values associated with fused results from preceding nodes along tributary routes. These values are conveyed by mobile software agents issued from preceding nodes. Therefore, our modification distributes the reputation (opinion) computation of the last fused result over the processing resources of the nodes along the route to the sink. This approach is equivalent to implementing a reputation-based security filter at each processing stage.

Integrating our temporal modification of reputation into the sensor-data fusion process improves the accuracy of intrusion detection and identification by reducing the false-alarm rate of the unsupervised technique of the probabilistic neural network (PNN). This PNN learns the signature of normal network traffic with the random weights typically used replaced by the trust-based quantified reputation of sensor data or subsequent aggregate information generated by our sequential implementation of a temporal version of Jøsang’s belief model.

The two-stage algorithm that detects network intrusions and subsequently identifies them (see Figure 2) overcomes the problems of large sensor-data loads and resource restrictions in WSNs. The first stage comprises a clustering algorithm that reduces the data payload to a tractable size. A neural-network (NN) algorithm based on the modified reputation model can be implemented using a system of mobile software agents that adapt to available resource capacities at the nodes to carry out the parallel distributed computations of successive reputation values. The revised algorithms reduce complexity, distribute storage use, and respond robustly to variability in sensor data. Dimensionality reduction caused by the NN clustering algorithms further reduces communication costs and energy consumption. The second stage uses a version of a support-vector machine (SVM) based on the modified reputation model. The algorithm’s efficiency is improved by the availability of knowledge about the sensor-data payload. Unsupervised-learning methods are applied to the SVM for classification of the intrusion attacks.

We assessed the performance of the two-stage algorithm in simulations of WSN scenarios with multiple sensors at edge nodes for known intrusion types: black hole, flooding, Sybil (using forged identities in peer-to-peer networks), and other denial-of-service attacks. Our simulation results demonstrate reduced response times of the two-stage design using reputation-based NNs to intrusion anomalies from both compromised nodes and

Continued on next page
external intrusion attacks. The time needed for anomaly detection is reduced by as much as 25%, while the average reduction in correct identification time is 10%. For the simulated scenarios the accuracy of the new approach is an increase of 22% over the earlier approach. In addition, the proposed classifiers based on the temporal and distributed modification of the original belief models and the associated reputation-based NNs disperse the short- and long-term memory of the sensor inputs.

In summary, we propose a reputation-based extension of neural algorithms for unsupervised detection and identification of anomalies in WSNs caused by intrusion attacks. The new classification routines function as security alerts when anomalous inputs are detected. The performance results for known intrusion types also reveal a complementary advantage: the framework based on the temporal and distributed modification of the belief models represents a powerful mechanism for quantification of uncertainty in WSNs. Future research will focus on the extent to which this approach can purge false data to accomplish robust information aggregation in the presence of an increasing number of compromised nodes.

Author Information

William S. Hortos
Associates in Communications Engineering Research and Technology
Orlando, FL

William Hortos is the founder of a consultancy in innovative radio-frequency and wireless technologies. He holds a PhD in electrical engineering from the University of Michigan. His research interests include adaptive and stochastic optimization, wireless communications and WSNs, neural and evolutionary computation, and real-time multimedia.

References