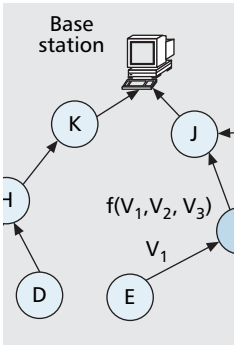
INTRUSION DETECTION TECHNIQUES IN MOBILE AD HOC AND WIRELESS SENSOR NETWORKS

BO SUN AND LAWRENCE OSBORNE, LAMAR UNIVERSITY
YANG XIAO, THE UNIVERSITY OF ALABAMA
SGHAIER GUIZANI, UNIVERSITY OF QUEBEC AT TROIS-RIVIERES



Mobile ad hoc networks and wireless sensor networks have promised a wide variety of applications. However, they are often deployed in potentially adverse or even hostile environments. Therefore, they cannot be readily deployed without first addressing security challenges.

ABSTRACT

Mobile ad hoc networks and wireless sensor networks have promised a wide variety of applications. However, they are often deployed in potentially adverse or even hostile environments. Therefore, they cannot be readily deployed without first addressing security challenges. Intrusion detection systems provide a necessary layer of in-depth protection for wired networks. However, relatively little research has been performed about intrusion detection in the areas of mobile ad hoc networks and wireless sensor networks.

In this article, first we briefly introduce mobile ad hoc networks and wireless sensor networks and their security concerns. Then, we focus on their intrusion detection capabilities. Specifically, we present the challenge of constructing intrusion detection systems for mobile ad hoc networks and wireless sensor networks, survey the existing intrusion detection techniques, and indicate important future research directions.

INTRODUCTION

Mobile ad hoc networks (MANETs) and wireless sensor networks (WSNs) are relatively new communication paradigms. MANETs do not require expensive base stations or wired infrastructure. Nodes within radio range of each other can communicate directly over wireless links, and those that are far apart use other nodes as relays. Each host in a MANET also acts as a router as routes are mostly multihop. The lack of fixed infrastructure and centralized authority makes a MANET suitable for a broad range of applications in both military and civilian environments. For example, a MANET could be deployed quickly for military communications in the battlefield. A MANET also could be deployed quickly in scenarios such as a meeting room, a city transportation wireless network, for fire fighting, and so on. To form such a cooperative and self-configurable network, every mobile host should be a friendly node and willing to relay messages for others. In the original design of a MANET, global trustworthiness in nodes within the whole network is a fundamental security assumption.

Recent progress in wireless communications and micro electro mechanical systems (MEMS) technology has made it feasible to build miniature wireless sensor nodes that integrate sensing, data processing, and communicating capabilities. These miniature wireless sensor nodes can be extremely small, as tiny as a cubic centimeter. Compared with conventional computers, the low-cost, battery-powered, sensor nodes have a limited energy supply, stringent processing and communications capabilities, and memory is scarce. The design and implementation of relevant services for WSNs must keep these limitations in mind. Based on the collaborative efforts of a large number of sensor nodes, WSNs have become good candidates to provide economically viable solutions for a wide range of applications, such as environmental monitoring, scientific data collection, health monitoring, and military operations [1].

An example WSN is illustrated in Fig. 1. In Fig. 1, the WSN is deployed to detect targets. After sensor nodes detect a target, they can collaboratively route data to a base station for analysis. Then, the base station can transmit data further to users through another communications infrastructure, for example, the Internet.

Despite the wide variety of potential applications, MANETs and WSNs often are deployed in adverse or even hostile environments. Therefore, they cannot be readily deployed without first addressing security challenges. Due to the features of an open medium, the low degree of physical security of mobile nodes, a dynamic topology, a limited power supply, and the absence of a central management point [2], MANETs are more vulnerable to malicious attacks than traditional wired networks are. In WSNs, the lack of physical security combined with unattended operations make sensor nodes

1536-1284/07/$20.00 © 2007 IEEE

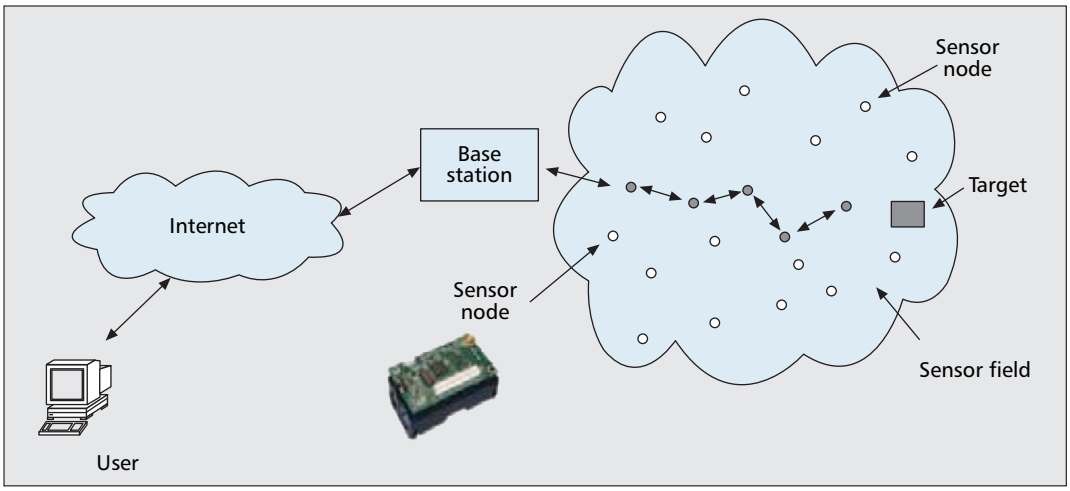


Figure 1. *An example of a wireless sensor network.*

prone to a high risk of being captured and compromised, making WSNs vulnerable to a variety of attacks.

So far, research to find security solutions for MANETs and WSNs has originated from the *prevention* point of view. For example, in both networks, there exist many key distribution and management schemes that can be built based on link-layer security architecture, prevention of denial of service attacks, and secure routing protocols. There is also research targeted to specific services and applications. For example, one of the most important purposes of deploying WSNs is to collect relevant data. In a data collection process, aggregation was required to save energy, thus prolonging the lifetime of a WSN. However, aggregation primitives are vulnerable to node compromise attacks. This leads to falsely aggregated results by a compromised aggregator. Hence, effective techniques are required to verify the integrity of aggregated results.

Prevention-based approaches can significantly reduce potential attacks. However, they cannot totally eliminate intrusions. After a node is compromised, all the secrets associated with the node are open to attacks. This renders prevention-based techniques less helpful for guarding against malicious insiders. In practice, insiders can cause much greater damage. Therefore, intrusion detection systems (IDSs), serving as the second line of defense, are indispensable in providing a highly-secured information system. By modeling behaviors of proper activities, an IDS can effectively identify potential intruders and thus provide in-depth protection.

In this article, we first provide a brief introduction to an IDS. Then, we present challenges in constructing IDSs for mobile ad hoc networks and wireless sensor networks and survey their existing intrusion detection techniques. Finally, we point out important future research directions.

Intrusion Detection Techniques

An intrusion is defined as a set of actions that compromises confidentiality, availability, and integrity of a system. Intrusion detection is a security technology that attempts to identify those who are trying to break into and misuse a system without authorization and those who have legitimate access to the system but are abusing their privileges. The system can be a host computer, network equipment, a firewall, a router, a corporate network, or any information system being monitored by an intrusion detection system.

An IDS dynamically monitors a system and users' actions in the system to detect intrusions. Because an information system can suffer from various kinds of security vulnerabilities, it is both technically difficult and economically costly to build and maintain a system that is not susceptible to attacks. Experience teaches us never to rely on a single defensive technique. An IDS, by analyzing the system and users' operations, in search of undesirable and suspicious activities, may effectively monitor and protect against threats.

Generally, there are two types of intrusion detection: misuse-based detection and anomaly-based detection [3]. A misuse-based detection technique encodes known attack signatures and system vulnerabilities and stores them in a database. If a deployed IDS finds a match between current activities and signatures, an alarm is generated. Misuse detection techniques are not effective to detect novel attacks because of the lack of corresponding signatures. An anomaly-based detection technique creates normal profiles of system states or user behaviors and compares them with current activities. If a significant deviation is observed, the IDS raises an alarm. Anomaly detection can detect unknown attacks. However, normal profiles are usually very difficult to build. For example, in a MANET, mobility-induced dynamics make it challenging to distinguish between normalcy and anomaly. It is, therefore, more challenging to distinguish between false alarms and real intrusions. The capability to establish normal profiles is crucial in designing an efficient, anomaly-based IDS.

As a promising alternative, specification-based detection techniques combine the advantages of misuse detection and anomaly detection by using manually developed specifications to characterize legitimate system behaviors. Specifi-

Intrusion detection is a security technology that attempts to identify those who are trying to break into and misuse a system without authorization and those who have legitimate access to the system but are abusing their privileges.

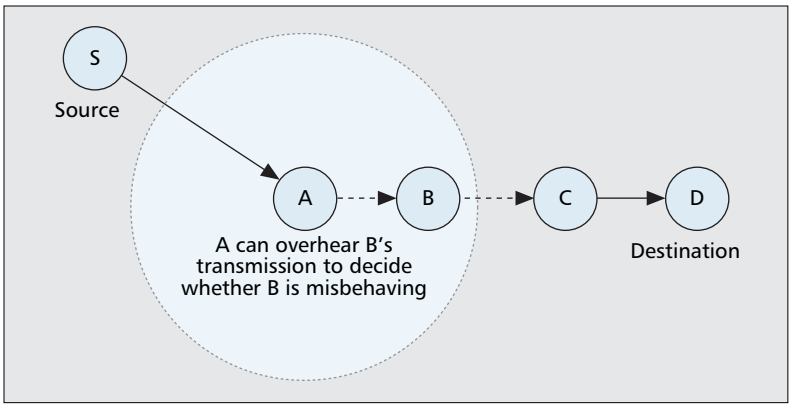


Figure 2. *Watchdog mechanism for MANETs.*

cation-based detection approaches are similar to anomaly detection techniques in that both of them detect attacks as deviations from a normal profile. However, specification-based detection approaches are based on manually developed specifications, thus avoiding the high rate of false alarms. However, the downside is that the development of detailed specifications can be time-consuming.

Intrusion Detection in a MANET

Attack Models

It is very challenging to present a once-for-all detection approach. The analysis of existing attack models can facilitate the extraction of effective features, which turns out to be one of the most important steps in building an IDS. The following are representative types of attacks in the context of a MANET IDS:

- *Routing Logic Compromise*: In routing protocols, typical attack scenarios include black hole, routing update storm, fabrication, and modification of various fields in routing control packets (for example, route request message, route reply message, route error message, etc.) during different phases of routing procedures. All these attacks can lead to serious dysfunction in a MANET.
- *Traffic Distortion*: This includes attacks such as packet dropping, packet corruption, data flooding, and so on. Motivated by their different objectives, attackers may take different actions to manipulate packets. For example, attackers may randomly, periodically, or selectively drop received packets to selfishly save power or intentionally prevent other nodes from receiving data.

In addition to these, attacks such as rushing, wormhole, and spoofing also have been discussed in the context of a MANET. Furthermore, it is not difficult to fabricate intrusions based on the combination of attacks mentioned previously.

Existing Research

The pioneer ID research in the context of a MANET appears in a series of works in [2–6]. In the system concept, an agent is attached to each node. Each node can perform intrusion detection and response functionality individually. One of the most important steps in IDS research is to construct effective features. Focusing on MANET routing protocols, Zhang *et al.* [2] use an unsupervised method to construct a feature set and select an essential set of features (e.g., distance to a destination, node moving velocity, the percentage of changed routes, the percentage of changes in the sum of hops of all routes, etc.) that have high *information gain*. Information gain is an important metric to measure the effectiveness of features. Features with high information gain can facilitate a constructed IDS to achieve desirable performance. Different routing protocols may result in different feature sets.

Intrusion detection can be formulated as a pattern classification problem, in which classifiers are designed to classify observed activities as normal or intrusive. In [2], based on an identified feature set, Zhang *et al.* apply two well-known classifiers, RIPPER and support vector machine (SVM) Light, to construct a suite of anomaly detection models. RIPPER is a decision-tree equivalent classifier for rule induction. By separating provided data into appropriate classes, RIPPER can compute rules for the system. SVM Light can produce a more accurate classifier when the data that is provided cannot be represented by the given set of features.

Because of the locality of one intrusion session, *post-processing* also is introduced to filter out false alarms. In post-processing, if there are more abnormal predictions than normal predictions in a predefined period of time, activities defined in this period of time are deemed abnormal. In this way, spurious errors that occur during normal sessions can be removed.

Because of the importance of feature selection in IDS research, Huang *et al.* [4] further introduce a new learning-based method to utilize *cross-feature analysis* to capture inter-feature correlation patterns. Suppose that L features, $f_1, f_2, \ldots, f_L$, are identified, where each f_i denotes one feature characterizing either *topology* or *route* activities. The classification problem to be solved is to create a set of classification model C_i: $\{f_1, \ldots, f_{i-1}, f_{i+1}, \ldots, f_L\} \rightarrow f_i$ from the training process. Here one feature f_i is chosen as the target to classify. Then, the classification model C_i can be used to identify temporal correlation between one feature and all of the other features. The prediction of C_i is very likely in normal situations. However, when there are malicious events, the prediction of C_i becomes very unlikely. Based on this, normal events and abnormal events can be distinguished.

Local detection alone is not sufficient because of the distributed nature of a MANET. Huang and Lee [5] further elaborate on mechanisms in which one node can collaborate with its neighbors and initiate a detection process over a broader range. This can provide not only more accurate detection results, but also more information in terms of attack types and sources. After fairly and periodically electing a monitoring node in a cluster of neighboring MANET mobiles, a cluster-based detection scheme is proposed. Each node maintains a finite state machine, with possible states of *Initial*, *Clique*, *Done*, and *Lost*. Based on the finite state

machine, a set of protocols, including a clique computation protocol, a cluster-head computation protocol, a cluster-valid assertion protocol, and a cluster recovery protocol are detailed. Resource constraint problems faced by a MANET are addressed when these protocols are designed.

Based on a specification-based approach to describe major functionality of Ad hoc On Demand Distance Vector (AODV) routing algorithms at data layers and routing layers, Huang and Lee [6] propose an extended finite state automaton (EFSA), where transitions and states can carry a finite set of parameters. In this way, the proposed EFSA can detect invalid state violations, incorrect transition violations, and unexpected action violations. The construction of EFSA can lead naturally to a specification-based approach. Based on a set of statistical features, statistic learning algorithms are then adopted to detect abnormal patterns from anomalous basic events.

Based on Dynamic Source Routing (DSR) protocols, Marti *et al.* [7] propose to install extra facilities, *watchdog* and *pathrater*, to identify and respond to routing misbehaviors in a MANET. In data transmission processes, a node may misbehave by agreeing to forward packets and then fail to do so. Consider the example illustrated in Fig. 2 to understand the *watchdog* approach. Suppose a path exists from a source node *S* to a destination node *D* through intermediate nodes *A*, *B*, and *C*. Node *A* can overhear node *B*'s transmissions. Node *A* cannot transmit directly to node *C* and must go through node *B*. To detect whether node *B* is misbehaving, node *A* can maintain a buffer of packets recently sent by node *A*. Node *A* then compares each overheard packet from node *B* with a buffered packet of node *A* to see if there is a match. A failure tally for node *B* increases if node *A* finds that node *B* is supposed to forward a packet but fails to do so. If the tally is above one threshold, node *B* is deemed to be misbehaving. Each node maintains a rating for each node it knows about in the network. Then, a path metric can be calculated by averaging the node ratings in the path. Pathrater [7] can then select the path with the highest metric. Marti *et al.* [7] also discuss several limitations of this approach, including limitations resulting from packet collisions, false reports of node misbehavior, and potential watchdog circumvention mechanisms.

Focusing on AODV routing protocols, Tseng *et al.* [8] propose a specification-based ID technique. A finite state machine (FSM) is constructed to specify correct behaviors of AODV, that is, to maintain each branch of a route request/route reply (RREQ/RREP) flow by monitoring all of the RREQ and RREP messages from a source node to a destination node. Then, the constructed specification is compared with actual behaviors of monitored neighbors. The distributed network monitor passively listens to AODV routing protocols, captures RREQ and RREP messages, and detects run-time violations of the specifications. A tree data structure and a node coloring scheme also are proposed to detect most of the serious attacks.

Sun *et al.* [9] propose using a Markov chain (MC) to characterize normal behaviors of MANET routing tables. A MC-based local detection engine can capture temporal characteristics of MANET routing behaviors effectively. Because of the distributed nature of a MANET, an individual alert raised by one node must be aggregated with others to improve performance. Motivated by this, a nonoverlapping zone-based intrusion detection system (ZBIDS) is proposed to facilitate alert correlation and aggregation [9], as illustrated in Fig. 3. Specifically, the whole network is divided into nonoverlapping zones. Gateway nodes (also called interzone nodes, i.e., those nodes that have physical connections to different zones) of each zone are responsible for aggregating and correlating locally generated *alerts* inside a zone. Intrazone nodes, after detecting a local anomaly, generate an alert and broadcast this alert inside the zone. Only gateway nodes can utilize alerts to generate *alarms*, which can effectively reduce false alarms. In a ZBIDS, the aggregation algorithm can reduce the false alarm ratio and improve the detection ratio. An alert data model conformed to intrusion detection message exchange format (IDMEF) also is presented to facilitate the interoperability of IDS agents. Based on this, gateway nodes can further provide a wider view of attack scenarios.

Considering that one of the main challenges in building a MANET IDS is to integrate mobility with IDSs and to adjust IDS behavior, Sun *et al.* [10] demonstrate that a node's moving speed, a commonly used parameter in tuning MANET performance, is not an effective metric to tune IDS performance under different mobility models. Sun *et al.* then propose an *adaptive* scheme, in which suitable normal profiles and corresponding proper thresholds can be selected *adaptively* by each local IDS through periodically measuring its *local link change rate*, a proposed performance metric that can reflect mobility levels. The proposed scheme is less dependent on underlying mobility models and can further improve performance.

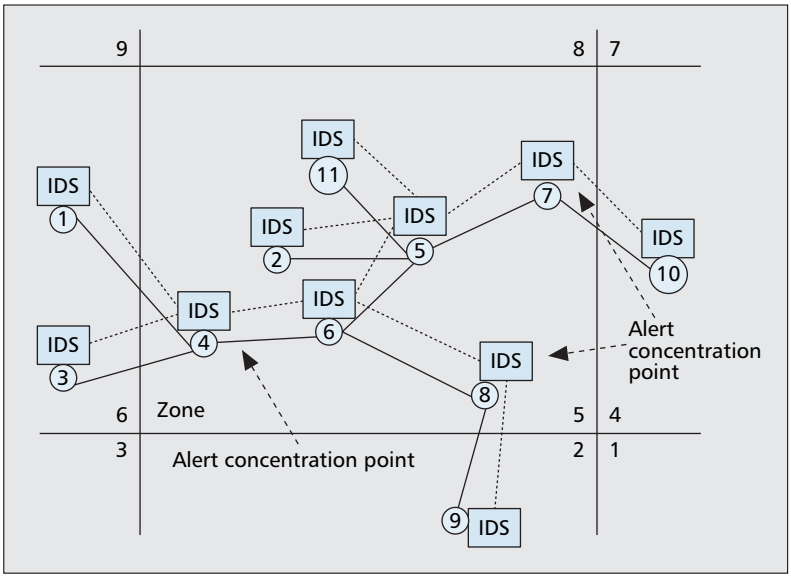


Figure 3. *The zone-based intrusion detection system for MANETs.*

Due to cost considerations, it is still not practical to equip every sensor node with a global positioning system (GPS) receiver. Therefore, many localization protocols have been proposed to help sensor nodes to estimate their locations.

Intrusion Detection in a WSN

Similar to security research in a MANET, many prevention-based approaches in a WSN have been proposed. These approaches address challenges including key establishment, trust set up, privacy, authentication, secure routing, and high-level security services. However, the large-scale decentralized deployment of a WSN and the lack of physical security make *prevention*-based schemes inadequate after sensor nodes have been compromised. Therefore, an IDS can also offer adequate security protection for a WSN.

In this section, we present a survey of existing IDS research in the context of a WSN. Compared with a MANET, a WSN provides a relatively newer communication paradigm. Therefore, there are fewer works that address the construction of a WSN IDS. Furthermore, different applications and services motivated by WSNs demonstrate different characteristics. Therefore, it is necessary to integrate ID approaches with corresponding applications because attacks targeted at different applications and services demonstrate different manifestations. In the following, we use two important services of a WSN, secure aggregation and secure localization, to illustrate current WSN IDS research efforts.

Challenges

The unique characteristics of sensor nodes pose challenges to the construction of a WSN IDS. A WSN has a limited power supply, thus requiring energy-efficient protocols and applications to maximize the lifetime of sensor networks. Sensor nodes have stringent system resources in terms of memory and computational capabilities, making intensive calculations impractical. Sensor nodes are prone to failure. This results in frequent network topology changes. Also, a WSN usually is densely deployed, causing serious radio channel contention and scalability problems. The design of an effective WSN IDS must bear in mind all of these challenges.

Secure Localization in WSNs

Many WSN applications require that sensor nodes have location information. Due to cost considerations, it is still not practical to equip every sensor node with a global positioning system (GPS) receiver. Therefore, many *localization* protocols have been proposed to help sensor nodes to estimate their locations. To utilize localization protocols, some special nodes, called beacon nodes, often are used. These *beacon* nodes are assumed to know their locations and transmit their locations to other non-beacon nodes through *beacon packets*. Non-beacon nodes also estimate certain measurements (e.g., received signal strength indicator) based on received beacon packets. Such measurements and the location information contained in beacon packets usually are referred to as *location references*. After non-beacon nodes collect enough location references, these nodes can then estimate their locations.

Localization protocols may become vulnerable when a WSN is deployed in a hostile environment. For example, beacon nodes may be compromised, thus providing incorrect information to mislead location estimation at non-beacon nodes. Therefore, secure location discovery services are required to ensure the normal operation of a WSN.

Utilizing deployment knowledge of a WSN and based on the fact that probability distribution functions of sensor locations usually can be modeled prior to deployment, Du *et al.* [11] propose that each non-beacon node can efficiently detect location anomalies by verifying whether estimated locations are consistent with the deployment knowledge. For example, if a group of sensor nodes are dropped out of an airplane sequentially as the plane flies forward, normal distributions can be used to model the deployment distribution of this group of sensor nodes. Each non-beacon node can compare its estimated locations with the deployment knowledge. If the level of inconsistency is above a predefined threshold, sensor nodes can decide that received location references are malicious.

Liu *et al.* [12] also propose a suite of approaches to filter out malicious location references. The first approach is based on minimum *mean square error*. Based on the observation that malicious location references and benign ones are usually inconsistent, non-beacon nodes can compute an *inconsistency* level of received location references. The inconsistency level is represented by a mean square error of estimation. If the mean square error is larger than a threshold, non-beacon nodes could think that the received set of location references is malicious. The second approach is the *voting-based location estimation* method. Specifically, the deployed area is divided into a grid of cells. The non-beacon node can then have every received location reference *vote* on the cells in which this node may reside and thus decide how likely this node is in each cell. After the voting process, the center of the cells with the highest votes may be used as the estimated location.

Secure Aggregation in WSNs

Aggregation has become one of the required operations for a WSN to save energy. One example of an aggregation tree is illustrated in Fig. 4. Nodes A, B, …, N denote different sensor nodes in WSNs, respectively. f denotes an aggregation function (average, sum, maximum, minimum, count, etc.). If node I is compromised, it can send false reports to node J. However, many existing schemes are designed without sufficient security in mind and cannot detect the above malicious behavior. Preventing this malicious behavior is the secure aggregation problem.

Based on statistical estimation theory, Wagner [13] introduces a theoretical framework to model and to analyze the resilient data aggregation problem. After concluding that commonly used aggregation functions are insecure, Wagner proposed using robust statistics for resilient aggregation. Finally, several general techniques, such as truncation (to place upper and lower bounds on an acceptable range of a sensor reading) and trimming (for instance, to ignore the highest 5 percent and the lowest 5 percent of sensor readings) are used to help improve the resilience of aggregation functions.

Combining prevention-based and detection-based approaches, Yang *et al.* [14] propose a Secure Hop-by-Hop Data Aggregation Protocol (SDAP) for WSNs. The design of SDAP is based on *divide-and-conquer* and *commit-and-attest* principles. Specifically, a probabilistic grouping method is used to *dynamically* divide nodes into multiple logical groups of similar sizes. In each logical group, a hop-by-hop aggregation is performed and one aggregate is generated from each group. This hop-by-hop aggregation is enhanced to ensure that each group cannot deny its committed aggregate. After receiving all the group aggregates, the base station can apply an approach based on the *Grubbs'* test to identify suspicious groups. This approach can help expunge outliers from received aggregates. Finally, each group under study must participate in the attestation process and prove the correctness of its group aggregates. After the attestation process, the base station can calculate the final aggregate over all the group aggregates that are either normal or have passed the attestation process.

Motivated by research in computer vision and automated cartography, Buttyán *et al.* [15] propose a random sample consensus (RANSAC) paradigm for resilient aggregation in a WSN. RANSAC is an outlier elimination technique that can handle a high percentage of outlier measurement data. Specifically, RANSAC uses as few non-attacked data as possible to determine an initial model. Assuming that the non-attacked data follow normal distributions, the RANSAC algorithm uses maximum likelihood estimation (MLE) to estimate the parameters of the initial model. After the initial model is decided, RANSAC tries to enlarge the initial dataset with consistent data. Outlier measurements can then be filtered out, even if a large quantity of sensor nodes is compromised.

Future Research Directions

In this section, we discuss future research directions to construct IDSs for both MANETs and WSNs.

In the system concept, IDS research for both MANETs and WSNs requires a distributed architecture and the collaboration of a group of nodes to make accurate decisions. ID techniques also should be integrated with existing MANET and WSN applications. This requires an understanding of deployed applications and related attacks to deploy suitable ID mechanisms. Attack models must be carefully established to facilitate the deployment of ID strategies. Also, solutions must consider resource constraints in terms of computation, energy, communication, and memory. This is especially important in the context of a WSN.

Extended Kalman Filter-Based Secure Aggregation for a WSN

In this section, we use secure in-network aggregation problems in a WSN as one example of how to create a lightweight ID mechanism [16].

In a WSN, consecutive observations of sensor nodes usually are highly correlated in time domains. This correlation, along with the collaborative nature of WSNs, makes it possible to predict future observed values based on previous values. Therefore, it is a viable approach to estimate aggregated in-network values, based on the normal profiles that can be constructed. However, in practice, due to high packet-loss rate, harsh environment, sensing uncertainty, and other issues, it is challenging to provide an accurate estimate for actual aggregated value. Also, the lack of time synchronization among children and parent nodes could make aggregation nodes use different sets of values for aggregation. The complexity of existing aggregation protocols also contributes to the challenges of modeling in-network aggregated values.

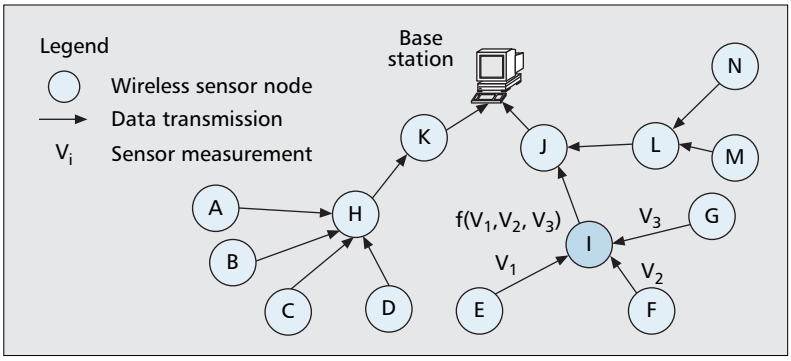


Figure 4. *An example aggregation tree in WSNs.*

To construct normal profiles for aggregated in-network values in the face of the previously mentioned challenges, solutions based on statistical estimation theory can be applied. Suitable models must consider the requirement of service and the application environment. For example, suppose that we are interested in estimating temperature values, which are scalar variables. We may adopt an extended Kalman filter (EKF) because an EKF can provide an accurate and lightweight estimation [16]. By enabling neighbor-monitoring mechanisms, each node can use an EKF to monitor the behavior of one of its neighbors. An EKF-based mechanism is suitable for WSN nodes, because this mechanism can address those incurred uncertainties in a lightweight manner and compute relatively accurate estimates of aggregated values, which based upon a normal range can be approximated. Utilizing a threshold-based mechanism, a promiscuously overheard value then is compared with a locally computed normal range to decide whether they are significantly different.

Furthermore, the monitored environment demonstrates spatial and temporal characteristics. Therefore, it is promising to integrate these characteristics into ID model construction. For example, there are existing works that model spatial and temporal properties of correlated data in a WSN. It is, therefore, desirable to integrate these models into the construction of normal profiles for in-network aggregated values. In this way, an anomaly-based ID service can be provided for secure aggregation in a WSN.

A WSN often is deployed to monitor emergency phenomena (such as the outbreak of a forest fire), about which good nodes can trigger

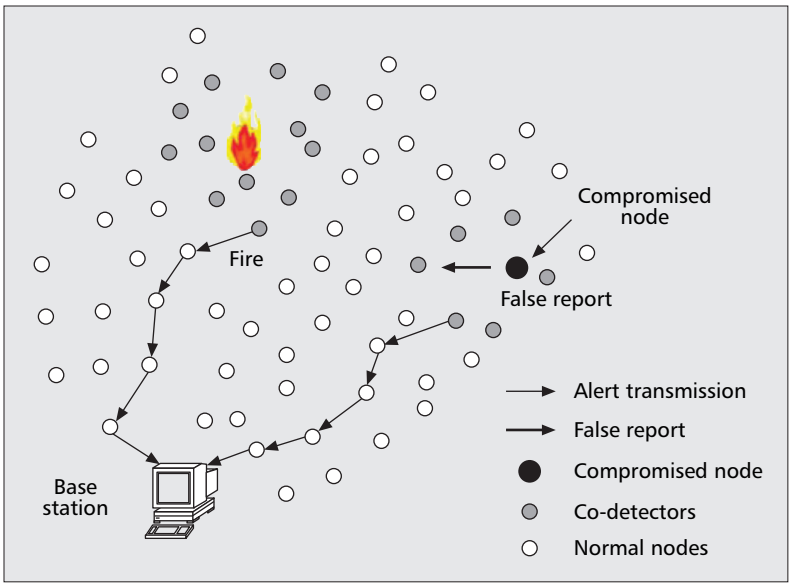


Figure 5. *Collaboration between IDM and SMM to differentiate malicious events from emergency events.*

important events and generate unusual yet important information. Node collaboration is necessary for sensor networks to make correct decisions about abnormal events.

Therefore, for WSNs, intrusion detection modules (IDM) and system monitoring modules (SMM) must integrate with each other to work effectively [16]. When node *A* raises an alert on node *B* because of an event *E*, to decide whether *E* is malicious or emergent, node *A* may initiate a further investigation on *E* by collaborating with existing SMMs. WSNs usually are densely deployed to collaboratively monitor events. To save energy, some sensor nodes are periodically scheduled to sleep. Based on this, node *A* can wake up those sensor nodes (denoted as co-detectors in Fig. 5) around node *B* and request from these nodes their opinions on the behavior of node *B* about event *E*. After node *A* collects the information from these nodes, if it finds that the majority of sensor nodes think that event *E* may happen, node *A* then makes a decision that *E* is triggered by some emergency events. On the other hand, if node *A* finds that the majority of sensor nodes think that event *E* should not happen, then node *A* thinks that *E* is triggered by either a malicious node or a faulty yet good node. To make a final decision, node *A* can continue to wake up those nodes around event *E* and request their opinions about event *E*. If node A finds that the majority of sensor nodes think that event *E* should not happen, node *A* then suspects that node *B* is malicious.

Integration of Mobility and Intrusion Detection in a MANET

One of the main difficulties in building MANET IDSs is to consider how mobility impacts the design of detection engines. This is especially important in the context of MANETs because most dynamics in MANETs are caused by mobility. MANET IDSs, without properly considering mobility, are prone to a high false positive ratio. This renders MANET IDSs less effective. *Link change rate* can be used to capture the impact of mobility on IDS engines. Based on the link change rate, a properly trained normal profile can be selected at different mobility levels *adaptively*. Using different mobility models, such as random waypoint model, random drunken model, and obstacle mobility model, an adaptive scheme is demonstrated to be less dependent on underlying mobility models and can further reduce the false positive ratio [16].

However, the performance of the proposed adaptive scheme at high mobility levels still is not as good as expected. It also is very challenging to construct mobility-independent MANET IDSs because this requires the extraction of mobility-independent features. Furthermore, how to systematically test the performance of MANET IDSs is still an on-going work.

Conclusion

Intrusion detection systems, if well designed, effectively can identify malicious activities and help to offer adequate protection. Therefore, an IDS has become an indispensable component to provide defense-in-depth security mechanisms for both MANETs and WSNs.

In this article, we provided an introduction to mobile ad hoc networks and wireless sensor networks and presented challenges in constructing IDSs for MANETs and WSNs. We then surveyed existing intrusion detection techniques in the context of MANETs and WSNs. Finally, using secure in-network aggregation for WSNs and the integration of mobility and intrusion detection for MANETs as examples, we discussed important future research directions.

Acknowledgment

This research was supported in part by the Texas Advanced Research Program under grant 003581-0006-2006 and the U.S. National Science Foundation (NSF) under grants DUE- 0633445, CNS-0716211, and CNS-0737325.

References

[1] I. F. Akyildiz *et al.*, "Wireless Sensor Networks: A Survey," *Elsevier Comp. Networks,* vol. 38, no. 2, 2002, pp. 393–422.
[3] H. Debar, M. Dacier, and A. Wespi, "A Revised Taxonomy for Intrusion Detection Systems," *Annales des Telecommun.*, vol. 55, 2000, pp. 361–78.
[2] Y. Zhang, W. Lee, and Y. Huang, "Intrusion Detection Techniques for Mobile Wireless Networks," *ACM Wireless Networks*, vol. 9, no. 5, Sept. 2003, pp. 545–56.
[4] Y. Huang *et al.*, "Cross-Feature Analysis for Detecting Ad-hoc Routing Anomalies," *Proc. IEEE ICDCS '03*, Providence, RI, May 2003, pp. 478–87.
[5] Y. Huang, and W. Lee, "A Cooperative Intrusion Detection System for Ad Hoc Networks," *ACM SASN '03*, Fairfax, VA, 2003, pp. 135–47.
[6] Y. Huang, and W. Lee, "Attack Analysis and Detection for Ad Hoc Routing Protocols," *Proc. RAID '04*, French Riviera, France, Sept. 2004, pp. 125–45.
[7] S. Marti *et al.*, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," *ACM Mobicom 2000*, Boston, MA, Aug. 2000, pp. 255–65.
[8] C.-Y. Tseng *et al.*, "A Specification-based Intrusion Detection System for AODV," *ACM SASN '03*, Fairfax, VA, 2003, pp. 125–34.
[9] B. Sun, K. Wu, and U. Pooch, "Alert Aggregation in Mobile Ad-Hoc Networks," *ACM WiSe '03* in conjunction with ACM Mobicom '03, San Diego, CA, 2003, pp. 69–78.

[10] B. Sun *et al.*, "Integration of Mobility and Intrusion Detection for Wireless Ad Hoc Networks," *Wiley Int'l. J. Commun. Sys.*, vol. 20, no. 6, June 2007, pp. 695–721.
[11] W. Du, L. Fang, and P. Ning, "LAD: Localization Anomaly Detection for Wireless Sensor Networks," *J. Parallel and Distrib. Comp.*, vol. 66, no. 7, July 2006, pp. 874–86.
[12] D. Liu, P. Ning, and W. Du, "Attack-Resistant Location Estimation in Sensor Networks," *ACM/IEEE IPSN '05*, Los Angeles, CA, Apr. 2005, pp. 99–106.
[13] D. Wagner, "Resilient Aggregation in Sensor Networks," *ACM SASN '04*, Washington DC, 2004, pp. 78–87.
[14] Y. Yang *et al.*, "SDAP: A Secure Hop-by- Hop Data Aggregation Protocol for Sensor Networks," *ACM Mobihoc '06*, Florence, Italy, 2006, pp. 356–67.
[15] L. Buttyán, P. Schaffer, and I. Vajda, "RANBAR: RANSAC-Based Resilient Aggregation in Sensor Networks," *ACM SASN '06*, Alexandria, VA, 2006, pp. 83–90.
[16] B. Sun *et al.*, "Integration of Secure In-Network Aggregation and System Monitoring for Wireless Sensor Networks," *IEEE ICC '07*, Glasgow, U.K., June 2007.

BIOGRAPHIES

BO SUN [M] (bsun@cs.lamar.edu) received his Ph.D. degree in computer science from Texas A&M University, College Station, in 2004. He is now an assistant professor in the Department of Computer Science at Lamar University. His research interests include the security issues (intrusion detection in particular) of wireless ad hoc networks, wireless sensor networks, cellular mobile networks, and other communications systems. His research is supported by the 2006 Texas Advanced Research Program and NSF DUE-0633445.

LAWRENCE OSBORNE (Lawrence.Osborne@lamar.edu) received an M.S. in mathematics from the University of Missouri Columbia in 1985 and a Ph.D. in computer science from the University of Missouri Rolla in 1989. He is now a professor of computer science at Lamar University, where he has worked since 1993. His research interests include algorithms for routing and localization in MANETs and wireless sensor networks, databases in sensor networks, satellite networks, and distributed systems. He is a co-principal investigator (Co-PI) on NSF DUE-0633445 with Dr. Bo Sun.

YANG XIAO (yangxiao@ieee.org) [SM] is currently with the Department of Computer Science at the University of Alabama. He was a voting member of the IEEE 802.11 Working Group from 2001 to 2004. His research areas are security, telemedicine, and wireless networks. His research has been supported by the U.S. National Science Foundation (NSF). He is a member of the American Telemedicine Association. He currently serves as Editor-in-Chief for International Journal of Security and Networks, International Journal of Sensor Networks, and International Journal of Telemedicine and Applications. He has served on the Technical Program Committees for more than 90 conferences such as INFOCOM, ICDCS, ICC, GLOBECOM, WCNC, and so on. He serves as an Associate Editor or on editorial boards for several journals, such as *IEEE Transactions on Vehicular Technology*.

SGHAIER GUIZANI (sghaier.guizani@umoncton.ca) obtained a Ph.D. in telecommunication from the University of Quebec, Trois-Rivières, Canada, an M.A.Sc. degree in electrical engineering from North Carolina A&T State University in 1992, and a B.Sc. from the State University of New York at Binghamton in 1990. He is currently working as an assistant professor at Qatar University in the Mathematics and Computer Department. His research interests are in the areas of optical fiber communication systems, radio over fiber, wireless network architectures, and wireless communication.