

Research challenges in lightweight intrusion detection for wireless sensor networks

Vijay Bhuse, *Student Member, IEEE*, Ajay Gupta, *Senior Member, IEEE* and Leszek Lilien, *Senior Member, IEEE*

Abstract— This short paper discusses our work in progress on intrusion detection (ID) in wireless sensor networks (*sensornets*). Its major goals are threefold. First, we discuss characteristics and vulnerabilities of sensornets that make necessary designing ID solutions specialized for sensornets. Second, we identify research challenges in ID for sensornets. Third, we propose initial ID solutions that exploit sensornet characteristics and take into consideration their resource-constrained nature. We also identify a new type of attack on sensornets, called *phenomenon forging*, and present solution ideas for it.

Index Terms— Sensor networks, sensornets, intrusion detection, IDS, security, DoS, phenomenon forging, anomaly detection, misuse detection.

I. INTRODUCTION

WIRELESS sensor networks (*sensornets*) are deployed for periodic monitoring of phenomena, or for detecting and reporting occurrences of specific events. Sensornet nodes are physically unguarded, resource-constrained and use wireless communication medium, which is susceptible to eavesdropping. This makes sensornets an easy target for attacks defeating the goals of their deployment, even without cracking cryptographic keys. As a consequence, the first line of sensornet defense, attack prevention, is not sufficient. The second line of defense, attack detection, using *intrusion detection (ID)* techniques is necessary.

There are many publications (e.g., [2, 11]) about possible *intrusion detection systems (IDS)* for a broader class of networks that includes sensornets, namely for *ad hoc networks (AHNs)*. But unless the IDSs are based on efficient mechanisms for detection of a sufficient variety of attacks, we will be far away from practical ID solutions. To the best of our knowledge, the efficient ID mechanisms for detecting intrusions other than packet dropping and flooding attacks in AHNs remain to be investigated. This means that the existing solutions for AHNs do not cover a sufficiently broad scope of intrusions.

In the next section, we present other reasons why even these IDSs for AHNs, for the limited set of intrusions, cannot be directly imported for sensornets. The most critical consideration in borrowing ID solutions from other AHNs is that energy resources in sensornets are even more constrained. Energy is an expensive resource for sensornets, because sensornet nodes use batteries. Recharging or replacing batteries is expensive and, depending on the deployment milieu, may even be impossible. To be practical for use in sensornets, solutions for detecting intrusions should be *lightweight*.

The next section discusses characteristics and vulnerabilities of sensornets that make general intrusion detection solutions for ad hoc networks infeasible for sensornets. Section III identifies research challenges in the

area of ID solutions for sensornets. The first challenge is to identify the most dangerous attacks on sensornets. We postulate that due to the limited sensornet resources, ID in a sensornet should be limited to only a few types of attacks most dangerous for sensornets. Then, we outline other research challenges that indicate the importance of designing *lightweight ID mechanisms for sensornets*. We also propose a few initial ID solutions that exploit sensornet characteristics. Section IV concludes the paper.

II. SALIENT FEATURES, VULNERABILITIES AND CONTROLS FOR SENSORNETS

Wireless sensornets can be viewed as a subcategory of wireless ad hoc networks. As such, the former must share some characteristics with the latter (like the use of the wireless medium) as well as have some distinguishing features. Salient features, listed below, make it difficult or impossible to simply import intrusion detection techniques for sensornets from AHNs.

A. Salient Sensornet Features vs. Ad Hoc Network Features

The distinct characteristics of sensornets vs. AHNs include the following:

1. Sensornet nodes are even more severely resource-constrained than AHNs. Uneven consumption of energy by sensornet nodes is a bigger problem. Partitioning in a sensornet is thus more probable, in effect seriously reducing the useful network lifetime.
2. In contrast to mobile AHNs, sensornet nodes are mostly stationary. (We consider stationary sensornets only.)
3. Both the coverage of the area to be monitored by a sensornet and the connectivity of its nodes must be taken into consideration during sensornet deployment [7]. This is not an issue for AHNs in general.
4. Traffic patterns in sensornets differs from traffic patterns in AHNs in at least the following ways:
 - a) Unlike in AHNs, traffic patterns in sensornets can be classified into three different categories [4]: many-to-one, one-to-many, or local communications. In *many-to-one communication*, many sensornet nodes send readings to a base station or an aggregation point in the network. Typically, data are aggregated on their way to the base station to reduce the number of messages [1]. In *one-to-many communication*, a single node (typically a base station or an aggregator) floods several sensornet nodes with a query or control information. Finally, in *local communication*, neighboring nodes send localized messages to discover each other and coordinate with each other.

- b) Traffic in sensornets is not as randomly distributed as in AHNs. Since sensornets are deployed to detect and report events to a base station, traffic is event-driven—which normally makes it bursty or periodic. Generally, the uneven traffic in sensornets makes defining its normal patterns difficult. Different routing protocols [3] and sleep-wakeup-based MAC protocols [10] take into consideration this nature of sensornet traffic.

B. Sensornet Vulnerabilities vs. Vulnerabilities of Ad Hoc Networks

Sensornets are more vulnerable to attacks than AHNs due to the following reasons:

1. Sensornet nodes are mostly physically unguarded. A capture of a single node by an attacker can result in a compromise of shared secrets or cryptographic keys.
2. Sensornet nodes are even more resource-constrained in terms of their radio range, processor speed, memory capacity and battery power.
3. DoS attacks can succeed more easily, since sensornet nodes are resource-constrained. Thus, DoS attacks are more dangerous, more easily defeating the purpose of sensornet deployment, even without cracking cryptographic keys.
4. Due to specific traffic patterns (as discussed above), use of asymmetric cryptographic primitives incurs a heavy communication overhead [8]. As a consequence, asymmetric cryptography—which is orders of magnitude slower than the symmetric one—is infeasible for data aggregation, considering limited resources of sensornet nodes.

C. Security Controls in Sensornets

Most common security controls used in all kinds of networks, AHNs included, are based on encryption. It is hard to imagine providing security controls for sensornets without cryptographic solutions, but—due to resource limitations in sensornets—these must be *lightweight* cryptographic solutions. Being lightweight, they will be even less effective than medium or heavyweight cryptographic solutions available for networks and AHNs, which are routinely complemented with ID systems.

Since lightweight encryption in sensornets will allow even more successful exploits, ID solutions are even more important in sensornets than in AHNs or other networks. At the same time, ID solutions for sensornets are even more difficult to devise due to their severe resource constraints.

In view of these facts, we postulate to limit intrusion detection in a sensornet to only a few types of attacks most dangerous for the sensornet. Details follow.

III. RESEARCH CHALLENGES IN

LIGHTWEIGHT INTRUSION DETECTION FOR SENSORNETS

This section identifies the major challenges in developing lightweight intrusion detection techniques for sensornets.

A. Challenge 1 and Initial Solutions

Challenge 1: Finding the most dangerous attacks by studying attack effects and finding attack precursors.

Simpler attacks on sensornets can be precursors leading to more dangerous ones. Figure 1 shows attack precursors for a number of common attacks. Detecting any of the precursors is a worthwhile goal as any simpler attack may precede more complicated and sophisticated attacks that are more difficult to detect. Finding precursors and detecting them as early as possible is also beneficial considering limitations on sensornet resources.

Attacks	Precursors
Masquerades	Packet forging or Sybil attacks
Sybil attacks	Packet forging
Man-in-the-middle attacks	Packet forging and masquerades
False route requests	Packet forging and attacking routing protocols
Misdirections	Packet forging
Selective forwarding	Packet dropping, sinkholes
Blackholes	Packet dropping

Figure 1: Attacks and their precursors

Major *effects* of these and other (less common attacks are briefly enumerated in Figure 2. It should be noted that to create a sinkhole, adversary attracts traffic towards itself. An attacker exploits weaknesses in the routing protocol to launch this attack. A sinkhole can be a precursor to other attacks, like selective forwarding.

Attacks	Effects
Physical capture, Tampering, Jamming, Collisions, Unfairness	Unavailability
Man-in-the-middle, Packet dropping, Blackhole, Selective forwarding	Network partition, Exhaustion
Sinkhole, Flooding, False route request, Misdirection, Wormhole	Exhaustion
Selective forwarding	Unavailability, Exhaustion

Figure 2: Attacks and their major effects

The following parameters can be used to quantify threats posed by attacks:

1. An immediate threat vs. a long-term effect: Some attacks may pose immediate threats to sensornet operations whereas some may not. The latter might still be very harmful in a long term if undetected.
2. Active vs. passive: Attacks may be active (e.g., packet forging) or passive (e.g., overhearing by adversary).
3. Amount of resources used by attackers: Some attacks may need quite resourceful attackers (e.g., HELLO flood attacks) or more than one attacker (e.g., DDoS), whereas others can be mounted even by nodes with just normal resources (e.g., blackholes).
4. Sensornet participation: Some attacks are possible only if an adversary joins the sensornet prior to attacking it.

It might be hypothesized that a higher priority in detection should be given to immediate threats, active attacks, attacks that need lesser resources, and attacks that do not need sensor participation. (As a consequence, attacks that do not pose immediate threats, passive attacks, attacks that require more resources, and the attacks that require sensor participation would be detected only as time and resources permit.) This hypothesis needs to be investigated.

Attacks leading to exhaustion do not pose an immediate threat but if undetected can decrease the network lifetime considerably. Since they do not pose an immediate threat, should their detection be done as time and resources permit? The attacks caused by packet forging lead to more dangerous and sophisticated attacks like man-in-the-middle. Attacks caused by packet dropping lead mainly to exhaustion of energy. But if a malicious node drops packets continuously, then its neighbors might wrongly conclude that it is dead. This may lead to network partitions.

Packet forging and packet dropping are the precursors to many dangerous attacks, as shown in Figure 1. We discuss next a few initial solutions for detecting some simple attacks that can also be precursors.

Initial Solution 1a—Detection of Packet Dropping

Paths: One of the most common solutions for detecting packet dropping [2, 5] in AHNs is to monitor every *node* in order to detect *nodes* dropping packets. A lightweight approach can be to monitor, detect and isolate *paths* that drop packets. Sensornets are generally dense, which means availability of redundant nodes and alternate paths in many areas.

The mechanism works as follows. Find during the route discovery process an alternate path that is node-disjoint with the original path. The alternate path can be used by the receiver *R* to send back to the sender *S* the number of packets that *R* received from *S*. If at least one node on the original path drops packets, *S* will see a number lower than its own count of packets sent by it to *R*. After detecting that the original path drops packets, an alternate path can be used for subsequent communications.

Initial Solution 1b—Detection of Sybil Attacks: In a Sybil attack, a node illegitimately assumes multiple identities. If undetected, this attack can be very dangerous for election algorithms, where a majority vote wins. If a masquerade can be detected, then a Sybil attack can also be detected. But detecting masquerades is an open research challenge. One solution for detecting a Sybil attack launched by a participating node is as follows. Suppose that *i* sensor nodes suspect that another node is posing a Sybil attack on them by assuming *k* identities. If $i < k$, they can ask $k - i$ other trustworthy nodes for help. The *k* nodes can now test the collective resources of all *k* identities of the suspected node as follows. Each of the *k* testing nodes simultaneously asks a different one of the *k* identities (suspected to be a single Sybil attacker) to solve *k* different puzzles in order to test the computational power of the processor of the suspected attacker. If the suspected node is posing a Sybil attack, and if it has resources comparable to other nodes in the sensornet, then to answer all *k* puzzles it will need a period about *k* times

longer than any of the testing nodes (assuming all puzzles require the same time to solve). Thus, it will fail the test.

Initial Solution 1c—Detection of Masquerades: A solution is to build *node profiles* for neighbors from the existing system data extracted across multiple network layers. Node profiles are used to detect anomalies. At the physical layer these data can be RSSI values, at the MAC layer they can be TDMA or sleep-wakeup schedules, and at the application layer they can be the round-trip time for bidirectional communication. If an adversary tries to masquerade as another node, it can be detected by comparing its behavior characteristics (obtained in the real time) to the stored profile of the impersonated node. A mismatch that is severe enough will identify a masquerade. Using profile data extracted at multiple layers provides a more robust solution.

Another solution for detecting masquerades is watchdog-based and is discussed in the next section on Challenge 2.

B. Challenge 2 and Initial Solutions

Challenge 2: *Identifying data, information or properties that watchdogs can monitor, and measuring the cost and effectiveness of watchdogs.*

Watchdogs have been proposed mainly for detecting packet dropping attacks [5, 6]. We propose using watchdogs to detect masquerade attacks. It is very important to identify the minimum amount of data, information or properties that watchdogs need to monitor to be able to detect a given number of attacks.

By monitoring packets, watchdogs can extract the following information and use it for attack detection:

1. The received signal strength indicator (RSSI) value for the signal, time of flight for a quick bi-directional communication, time of transmission or reception for a packet, or other physical, temporal and spatial properties of the received packet.
2. Nodes receiving a given packet or at least the network area that receives the packet.
3. Application-specific information that can be used to detect intrusions. Examples are a timestamp or a location of a network area where a query needs to be performed.

Design of watchdog-based detection mechanisms should take into account the following important issues and criteria:

1. Watchdogs may need to observe a certain minimum number of packets to detect an attack.
2. Some watchdogs may need continuous monitoring whereas others may need periodic monitoring. The latter are preferable for resource-constrained sensornet nodes.
3. Watchdogs may monitor the behavior of nodes, paths or clusters. Watchdogs that can detect attacks by just observing end-to-end behavior of a path are preferable over watchdogs that need to monitor every single node.
4. Current watchdog-based mechanisms [5] assume that the area in which a signal can be received is circular, with the transmitting node at the center of the circle. In practice the area is not circular. Watchdog-based mechanisms should be designed to adapt to the actual area shapes of radio ranges.

5. Some detection techniques may require collaboration among watchdogs [6]. In such cases, providing a secure channel of communication between watchdogs is necessary. Providing it in the presence of attackers is a challenge.
6. Collisions and hidden nodes pose problems to watchdog-based mechanisms and result in a large number of false alarms and misses [5].

Initial Solution 2a — Detection of Masquerades: Researchers have already proposed [5] watchdog-based mechanisms that exploit broadcast media to detect packet-dropping attacks in AHNs. Sensornet nodes may detect more attacks through a passive listening.

As an example, we propose a watchdog-based mutual guarding mechanism to detect masquerades. We assume that nodes are static and new nodes do not join the sensornet. Let $N(X)$ be the set of neighbors of node X . The steps in our watchdog-based mutual guarding solution are as follows:

1. Every node finds its neighbors (this information may be obtained during sensornet setup).
2. A node X can overhear and detect any of its neighbors masquerading as X , because the radio ranges overlap.
3. If node X overhears an outsider masquerading as a node Z that is not its immediate neighbor (Z is not in $N(X)$), X can detect the masquerade attempt. The reason is that the real node Z is too far away to be heard by X . X can be either the destination node or any node on the route.

Node density, radio ranges and topology are some of the important parameters that can affect the number of false alarms and misses.

C. Challenge 3

Challenge 3: *Informing the network about locally detected intrusions.*

Even though intrusions are detected at nodes running host-based IDSs, informing either the whole network or a part of the network about the intrusion or quarantining the misbehaving nodes is a challenge because of the following reasons:

1. It is costly to provide a secure channel of communication for a resource-constrained sensornet. This is the case even with lightweight cryptographic algorithms having low computational intensity.
2. Capture of a single sensor node results in compromising a shared cryptographic key. This is much more probable in sensornets than in AHNs in general since sensornet nodes are typically physically unguarded.
3. The adversary can eavesdrop on the wireless medium and can extract and misuse information shared between watchdogs. (Lightweight encryption can help.)

One more question remains open. If a secure communication channel cannot be provided, how can local ID information be shared among sensornet nodes in such a way that adversary gets either no or only a part of the useful information (and, in the latter case, cannot use it to pose any further attacks on the network)?

The number of adversaries present in the area and their locations will have a significant impact on the solutions.

D. Challenge 4 and Initial Solutions

Challenge 4: *Identifying types of DoS attacks specific to sensornets and proposing lightweight detection mechanisms.*

Sensornets are especially vulnerable to DoS attacks (e.g. exploiting buffer overflows) because sensornet nodes are resource-constrained. Security primitives based on cryptography are not sufficient to guard against DoS attacks because some DoS attacks can defeat the goal of the sensornet even without cracking its keys. As an example, consider phenomenon forging defined below. Apart from that, DoS attacks can target proposed MAC [10] and routing protocols [3] for sensornets.

Phenomenon Forging: Suppose that a sensornet is deployed to detect wildfires. Upon receiving an alert (which may contain a detection of a wildfire and its location), the response mechanism to extinguish wildfire gears up. An adversary can defeat the goal of the sensornet by fooling many sensors with small “deceptive” fires (depending on the sensornet intelligence, each could be just a lit match). In this way, the adversary can confuse the sensornet with false alarms and exhaust sensornet resources as well as the resources of the response mechanism. If a real wildfire starts after resource exhaustion, the sensornet and the response mechanism might be unable to adequately respond. We call this attack *phenomenon forging*. It is specific to sensornets, and it can be launched without cracking cryptographic keys or forging even a single data packet (the packets are all real – only the phenomenon is not).

Initial Solution 4a—Detection of Phenomenon Forging: To prevent sophisticated attacks, solutions should be designed carefully by taking into consideration the actual *application* of a given sensornet. Generic solutions will always leave some loopholes for an adversary to exploit. For our example, a simple solution can be to put a threshold on the number of nodes in an area that must detect a fire at approximately the same time. Since a single mobile adversary attacking a sensornet takes time to move from one sensor to another, the phenomenon-forging attack can be detected. Still, a gang of well-synchronized attackers can defeat this solution.

Initial Solution 4b—Detection of Invalid Information Source: Sensornets have specific communication patterns. Taking this into consideration, an adversary can try to infuse packets into the network. Suppose that Node X has four neighbors E , W , S and N . X receives from Node E data collected from the nodes that are situated in the eastern part of the sensornet. Similarly, X receives data from W , S , and N —for the western, southern and northern part, respectively. If X sends a query about temperature to the eastern part but it receives a reply from node other than E , then X will be suspicious about the originator of the packet. For any node, our proposed technique maps neighbors’ replies to the geographical location of the node that should directly reply to the X ’s query. If the reply comes to X from a neighbor from whom it is not supposed to come from, then X guesses that it is an attack infusing malicious packets.

Other ways of infusing packets remain unexplored. E.g., consider the phenomenon forging attack. When a sensor node detects a wildfire, it reports the presence and the location of the wildfire. The packet containing this information is sent to the base station. By forging just the location of the wildfire in the packet, an adversary might cause a lot of harm (such as diverting the response team)

E. Challenge 5

Challenge 5: *Detecting and identifying resources employed by an adversary.*

Detecting strength of an attacker is important because it can affect the reaction of the response mechanism. The resources employed by an adversary can be measured by:

1. Counting the number of attackers.
2. Investigating resourcefulness of each attacker.
3. Investigating the way the attackers communicate with each other. Well-connected attackers are more powerful.

Launching some attacks requires more effort. For example, an adversary wishing to create a sinkhole needs to participate in routing and find a loophole in it. A packet-dropping attack requires less effort.

Initial Solution 5a—Detection of a HELLO Flood:

A HELLO flood can be detected if nodes detect that the strength of the radio signal from an adversary is too high for a normal sensor node. The RSSI values and the area that receives a signal sent from an attacker can be used to classify the attacker as, for example, a mote-class or a laptop-class adversary [4].

F. Challenge 6

Challenge 6: *How to detect physical node capture and code tampering.*

Code tampering is very difficult to prevent without a special hardware (incl. a processor) and a compiler [ZC04 GN04]. Sensor network nodes are envisioned to become cheaper and smaller, eventually dust-sized [9]. They will be deployed in millions. To keep the costs low, it may not be possible to provide special hardware capabilities for such numerous and small nodes. This makes prevention of tampering difficult.

Since sensor network nodes are physically unguarded, a physical capture is easy. Capture of a node can compromise shared secrets and keys.

Initial Solution 6a—Detection of Physical Capture:

A physical node capture can be detected if nodes monitor the presence of their neighbors. Suppose, that it takes T seconds to physically capture a node, to reverse-engineer it, to modify its code, and to put it back at its original location. If nodes monitor the presence of their neighbors periodically every $t < T$ seconds, then a physical capture can be detected. This mechanism involves an overhead of periodic monitoring.

IV. CONCLUSIONS

Our contributions to intrusion detection for sensor networks can be summarized as follows:

1. We identified the specific properties of sensor networks that separate them from ad hoc networks and make it

difficult to directly import intrusion detection solutions from ad hoc networks.

2. We proposed techniques to rank threats posed by attacks on sensor networks. We described the relationships between attacks and their precursors, and the effects of attacks on sensor networks.
3. We proposed using watchdogs for detection of masquerades and packet dropping attacks. We identified information that watchdogs can obtain.
4. We indicated the importance of securely informing the whole network or a part of it about locally detected intrusions.
5. We identified a new type of DoS attack, named *phenomenon forging*, which is specific to sensor networks.

Our future work will involve proposing and analyzing—within the unifying framework of intrusion detection—lightweight solutions to problems discussed in this paper.

ACKNOWLEDGEMENTS

This research was supported in part by the National Science Foundation, under grants ACI-0000442, ACI-0203776, IIS-0242840 and MRI-0215356. Any opinions, findings, conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the funding agencies or institutions.

REFERENCES

- [1] M. Handy, M. Haase and D. Timmermann, "Low energy adaptive clustering hierarchy with deterministic cluster-head selection," *Proc. IEEE Intl. Conf. on Mobile and Wireless Communications Networks*, Stockholm, Sweden, Sept. 2002.
- [2] Y. Huang and W. Lee, "A Cooperative Intrusion Detection System for Ad Hoc Networks," *Proc. ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN '03)*, Fairfax, VA, Oct. 2003.
- [3] C. Intanagonwiwat, R. Govindan and D. Estrin, "Directed Diffusion: A Scalable and Robust Communication Paradigm for Sensor Networks", *Proc. Mobile Computing and Networking*, **CITY, STATE**, Aug. 2000, pp. 56-67.
- [4] C. Karlof and D. Wagner, "Secure Routing in Sensor Networks: Attacks and Countermeasures," *Ad Hoc Networks, Special Issue on Sensor Network Applications and Protocols*, vol. 1(2-3), Elsevier, Sept. 2003, pp. 293-315.
- [5] S. Marti *et al.*, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," *Proc. 6th Annual Int'l. Conf. on Mobile Computing and Networks*, Boston, MA, Aug. 2000, pp. 255-65.
- [6] P. Michiardi and R. Molva, "CORE: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," *Proc. Sixth IFIP Conf. on Security Communication, and Multimedia*, Portorož, Slovenia, Sept. 2002. **← [pages? (as for most others)]**
- [7] V. Mhatre, C.P. Rosenberg, D. Kofman, R.R. Mazumdar, and N. B. Shroff, "A Minimum Cost Surveillance Sensor

- Network with a Lifetime Constraint," *IEEE Trans. on Mobile Computing*, vol. 4(1), Jan. 2005, pp 4-15.
- [8] A. Perrig, R. Szewczyk, V. Wen, D. Cullar and J.D. Tygar, "SPINS: Security protocols for sensor networks," *Proc. MOBICOM*, Rome, Italy, July 2001, pp. 189-199.
- [9] W. Warneke and S. Bhave, "Smart Dust Mote Core Architecture," Project Report, Berkeley Sensor and Actuator Center, Berkeley, CA. Available at: <http://bwrc.eecs.berkeley.edu/Classes/CS252/Projects/Reports/warneke.pdf>
- [10] W. Ye, J. Heidemann and D. Estrin, "An Energy-Efficient MAC Protocol for Wireless Sensor Networks," *Proc. IEEE Infocom*, New York, NY, June 2002, pp. 1567-1576.
- [11] Y. Zhang and W. Lee, "Intrusion Detection in Wireless Ad Hoc Networks," *Proc. 6th Int'l. Conf. on Mobile Computing and Networks* ←[is my update correct?], Boston, MA, Aug. 2000, pp. 275-83.