VULNERABILITY OF INSENS TO DENIAL OF SERVICE ATTACKS

Kashif Saghar, David Kendall**

*School of Computing, Engineering and Information Sciences, Northumbria University, Newcastle upon Tyne, UK

Ahmed Bouridane†*

†College of Computer and Information Sciences, King Saud University Riyadh, Kingdom of Saudi Arabia

ABSTRACT

Wireless Sensor Networks (WSNs) may be deployed in hostile or inaccessible environments and are often unattended. In these conditions securing a WSN against malicious attacks is a particular challenge. This paper proposes to use formal methods to investigate the security of the INSENS protocol, in respect of its capability to withstand several denial of service attacks. The paper is an extension to our previous work where we proposed a formal framework to verify some wireless routing protocols. We have confirmed that the bidirectional verification employed by INSENS prevents attacks such as hello flood. However, INSENS is shown to be vulnerable to invisible node, wormhole and black hole attacks, even in a network of only a few nodes communicating over ideal channels. Packet loss in the presence of these attacks has been demonstrated and quantified using the TOSSIM wireless simulator.

Index Terms— Formal Modeling, Wireless Sensor Networks (WSN), Routing Protocol, Security Attacks.

1. INTRODUCTION

One of the main threat to WSNs is the denial of services (DoS) attacks that involve disrupting the routing and prevent data generated from sources to reach destinations. Some example of DoS attacks are black hole, hello flood, invisible node attack (INA) and wormhole attacks. One notable solution aimed at addressing the multiple DoS attacks is INSENS [2, 3]. The enhanced INSENS [3] protocol is an update of the basic protocol [2] in which multiple base stations (BSs) and multiple paths from sources to sinks are employed to improve the robustness. It also employs bidirectional verification in order to avoid hello flood and rushing attacks. Each sensor node employs four types of key: an individual key (shared with the base station); a pair-wise key (shared with a single neighbour); a cluster key (shared with all neighbouring nodes); and a group key shared by all the nodes in the network. The bidirectional phase involves exchanging two messages echo and echoback encrypted with the global key. Future messages are then accepted from the verified neighbours. One way hash chains are later used to provide message authentication both in route propagation (request message) and data routing. By applying the public hash function it can be confirmed that the message is new and has originated from the base station. These features enable INSENS to be one of the most secure routing protocols presented within the WSN community. The readers interested in INSENS may refer to [2] and [3] for a complete exposition.

We have used model-checking (UPPAAL) to investigate the resilience of the INSENS protocol to a variety of denial of service attacks. Model-checking can analyze a protocol exhaustively and thus determine the worst cases and hidden errors/bugs, which cannot otherwise be detected using other methods. We have also checked that our verification results can be observed empirically, using the wireless simulator TOSSIM. We can confirm that bidirectional verification addresses attacks such as hello flood and rushing. However, the protocol remains vulnerable to the invisible node attack (INA), wormhole, and black hole attacks, even in a network of only a few nodes communicating over an ideal channel with minimal collisions and multiple available paths. The rest of this paper is organised as follows: Section 2 briefly discusses related works; the method we adopted to verify different routing protocols is summarised in Section 3; the results of our formal framework that vulnerabilities of INSENS to different attacks is described in Section 4; conclusions and further work are presented in Section 5.

2. RELATED WORK

It has been acknowledged by the research community that computer simulations are often inadequate for finding bugs in routing protocols. Therefore, the development of formal models to analyze and verify various aspects of routing protocols is becoming increasingly important. Formal models have also been used in the analysis of security attacks. Different hidden attacks have been discovered using formal modeling, for example in TinySec and LEAP protocols by [9]; SNEP protocol by [8]; μTESLA and LEAP protocols by using SPIN [4]; and DoS attacks on Dynamic Source Routing (DSR) in [1]. We earlier verified some routing protocols against DoS attacks in [5, 6, 7] and show their vulnerabilities to these at-

tacks. The work in this paper further extends our initial work and presents a solution RAEED to rectify a DoS attack, black hole, by rigorously checking it using formal modelling.

3. THE FORMAL FRAMEWORK

The method adopted is a combination of formal modelling and computer simulations. A given routing protocol is converted into a formal model (we call it formal framework) and specification properties defined to check the presence of any faults (vulnerability to attacks) present in the routing protocol. The properties included basic *sanity* checks (confirmation that the model possesses some fundamental properties, debugging checks, etc.), the *liveness* (something good will eventually occur) and the *safety* (nothing bad ever occurs). In case a property fails, the formal model-checker automatically generates a trace providing the reason as to how the attack occurred in the protocol. The results are then confirmed and quantified using computer simulations.

The formal framework comprises 5 main parts: attacker model, sink model, channel model, event generator (EG) model and node models. The protocol is checked against different DoS attacks independently, thus the *attacker model* is replaced for each specific attack. A *black hole* is modelled simply by modifying the node model which forwards all messages correctly except data messages.

The *channel model* represents the topology and the capacity for communication between both legitimate (including BS) and malicious nodes. In UPPAAL node connectivity (RF links) is modelled using a NxN topology matrix with 1 or 0 in matrix indicate existence or absence of a an RF link, where N is the total number of nodes in a network.

The *node* model contains a number of states depending on the protocol's specifications. Each particular message passed between nodes in a protocol enables at least 2 states in the node model 'send' and 'receive'. Sometimes more than 2 states are needed, e.g. before sending the data from the source node a 'sense' state models sensing data from environment. Apart from these states there is always a state in which a node does nothing and remains idle (listen state). Some other states in the node model are the 'finish' and 'initial' states, indicating the starting and the terminating states of a protocol. Multiple concurrent node models are used in the formal framework because WSN comprised of more than one node. The node can be a source, a target, the destination or relay (intermediate) depending upon particular routing protocol requirements. The *base station (BS)* or *sink* is also a node. But in order to save the state space, the framework models it separately from the node model. The node model for INSENS is composed of 4 phases: (i) pair keys are exchanged by echo beacons; (ii) cluster keys are unicasted to all verified neighbours; (iii) request message is flooded by the base station (BS); and (iv) data is unicasted by the source node.

Finally the *event generator model* is used to generate different events required in the protocol. The events are triggered to enable the nodes to sense data from environment, to generate a timer's timeout or to complete a particular phase.

4. RESULTS OF FORMAL FRAMEWORK ON INSENS

In this paper we assume that a channel is ideal and no message is lost due to collisions or noise. The attackers are modelled independently and the protocol is checked for one attack at a time except for the INA and wormhole attacks which are checked along with the black hole attack. It is assumed that any node within an attacker's range can be attacked. Moreover it is assumed that INA, wormhole and hello flood attackers are deployed before Phase 1; while the black hole attack can be deployed during any phase. Our formal model has confirmed that INSENS can solve hello flood and sink hole attacks, however INSENS is still vulnerable to wormhole and INA attacks in phases 1&2 and when new nodes are deployed at a later stage. Moreover, a black hole attack is possible after the node is compromised or success of the wormhole/INA at any stage. These results are explained in detail in following sections.

4.1. Invisible Node Attack (INA)

All 5-node network topologies with 2 multiple paths were checked. The model confirmed that in most topologies data does not reach the BS in the presence of an INA even if a legitimate path exists. To check for additional multiple paths, a 9 node network was employed. As checking all possible topologies (2^{36} combinations) for 9 nodes is much more computationally demanding than for 5 nodes (2^{10} combinations), only a square grid node placement was checked. An error in a 9 node network was disclosed due to an INA even in the presence of 8 multi-paths. The theorem checked was the liveliness property that after the source node has sensed the data it leads to the sink receiving that data.

The issue of the data not reaching the BS, due to the addition of unconnected nodes in the verified neighbour list of the source and the other nodes was subsequently investigated. In order to check the success of an INA one needs to model only the echoback part (Phase 1) of the protocol. The reason being INA and wormhole attack will remain unsuccessful if they are unable to create virtual links in the Phase 1. The messages are only accepted from verified neighbours after Phase 1. The check is a safety property claiming that a source node possesses fewer than *N* unconnected nodes in its verified neighbour list.

To confirm this result the same network topology was developed and tested using the TOSSIM simulator. However, the encryption/decryption operations and the message authentication code (MAC) were simplified. As the attacker need not know about the encryption details, the CBC mode technique

was not used to generate the MAC (block cipher algorithm RCA) as in the INSENS protocol. The emphasis of this research does not concern these encryption techniques so these were not implemented.

The developers of INSENS do not explain how the data will flow towards the BSs. However, they do refer to forwarding data back to the nodes from which they received their first request beacon (parent nodes). In order to test the INSENS we employ data forwarding towards parent and random neighbour forwarding. The simulation were run both in the presence and the absence of INA. The attacker affected the data throughput in all cases, however, maximum damage was done when the attacker was not on the boundary of the grid. The data was sent periodically from the source to a single BS for a total of 1000 times and the BS maintained a record of the received data using the message ID attached to each message. Each experiment was repeated 20 times.

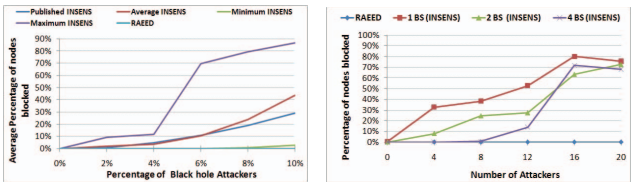
A 9 node network (3x3 grid), for which our formal framework detected a successful INA, was implemented. The simulation results confirmed that if the data was sent through the parent nodes, the data delivery percentage at the BS was reduced to 0%. This is because the links via an INA will always be marked as the parents (provides the shortest path) for all nodes within the source node's range. In the case of random selection, throughput was reduced to 10% on average [range: 4% to 17%] even if 8 multiple paths were used. (INA will enable 8 paths in this network). Thus, the simulation results confirmed that the formal framework correctly detected INSENS being vulnerable to the INA.

4.2. Wormhole Attack

It has been pointed out in the Section 4.1, that using the bidirectional verification phase of the model, one can check in which topology a wormhole attack will have a detrimental effect. Later, networks of 25 and 36 nodes placed in regular grids of (5x5) and (6x6) were checked. It was confirmed that the Uppaal model always detected virtual connections. The same topologies were checked using TOSSIM as was done for the INA. It was confirmed that the data delivery rate reduced dramatically in the presence of a wormhole, even with multiple paths (up to 8). For 36 node network, the percentage of data reaching the BS was reduced to 0% in case of parent selection. Again, as with the INA, all nodes will mark the nodes via the wormhole tunnel as their parent. If nodes are randomly selected, the average throughput of data reaching the BS was reduced to 2% on average [range: 0% to 6%] in the presence of a wormhole.

4.3. Black Hole Attack

Formal analysis and simulation have been applied also to an investigation of the black hole attack. The formal framework confirmed that black hole was successful in INSENS in Phase 4 when nodes transmit data back to the BSs. Apart from checking all possible 5 nodes networks a 25 node network (5x5 grid) and with 2 BSs positioned at opposite corners. The liveliness property was modified since receiving the data at either of the two BSs or sinks was acceptable. It was found that liveness property was violated when the number of attackers was increased to 2, each being placed near the individual BSs.



(a) 1000 node network (b) 200 node network

Fig. 1. Percentage of nodes blocked due to black hole attack on INSENS and RAEED protocols

The 25 node network was later implemented in TOSSIM in the presence of 2 and 4 BSs. The number of attackers and paths were also kept equal to the number of BSs for this network. The average percentage of the data reaching the BS was 80% [range: 38% to 100%] (2 BSs; 2 attackers; 2 paths) and 55% [range: 44% to 72%] (4 BS; 4 paths; and 4 attackers). This percentage reduced in the presence of 4 BSs because 4 attacker nodes were deployed in this case. The black hole attack was further tested with 4 BSs, 4 attackers and 100 nodes in 10x10 square grid. BSs were located one at each corner of the grid. With a density of 8 neighbours the average delivery percentage was 37% [range: 16% to 61%] and 5% [range: 1% to 18%] in the presence of 4 and 8 attackers respectively. However, by increasing density to 20 neighbours the average throughput improved to 80% even in the presence of 8 attackers.

4.4. A solution to INSENS problems: RAEED

We have developed a new routing protocol RAEED to address the issues/weaknesses present in INSENS protocol. We have applied a 'Neighbourhood watch' approach to allow nodes to detect path failures and to allow for alternative path selection. This provides a solution to the black hole attack to some extend and increase throughput. The simulation results against black hole attack is shown in Figure 1(a)and 1(b) for 200 nodes and 1000 nodes network. It is evident that number of nodes blocked due to black hole attack is negligible in RAEED protocol as compared to INSENS. We also applied a solution to solve attacks such as wormhole and INA before Phase 1 and during new nodes deployment. Our framework has shown that the new solution gives improved results as compared to INSENS. We later support these formal mod-

elling results with the computer simulations. These results are the subject of further work and we aim to publish those results later.

5. CONCLUSIONS AND FUTURE WORK

We have developed a formal framework that can detect vulnerability of a wireless routing protocol against DoS attacks [5, 6, 7]. This efficient bug hunting technique can find worst cases and hidden errors automatically. Thus any case of a protocol being vulnerable to a particular DoS attack is exposed and a trace showing how and why that attack is successful is generated automatically. The current paper is further extension of that work and applies formal modelling to a more robust protocol INSENS

The developers of INSENS claim that the enhanced INSENS protocol, because of the presence of multiple paths, is immune from the denial of service (DoS) attacks. Our formal modelling and simulation results refute this. We have successfully demonstrated that INSENS is indeed vulnerable to some DoS attacks such as INA and wormhole attack even in presence of an ideal channel (with minimum collision and no noise), with the availability of multiple paths and in small networks. Once a wormhole has successfully been launched, a rushing attack can easily be launched during the request propagation period. We confirm that if the INA and wormhole are deployed after Phase 1 these attacks can be defeated. This assumption may not be true in the real world because attackers might be present before the node deployment. Moreover, there is always the scenario when new nodes are deployed which will be then always be vulnerable to INA and wormhole attacks.

We have also confirmed that the black hole attack can cause a low throughput, especially in low density networks. We have checked that even with a network density almost the same as that employed in [3] and with a low percentage of attackers, many messages can be blocked during the data forwarding period if attackers are near each sink even under ideal conditions. We expect this to be a further reduced in larger networks (with the same density) with the same percentage of attackers, as more messages will pass through these attackers. (if the percentage of malicious nodes remains the same, the number of attackers will increase with network size). We have checked the effect of the black hole attack under ideal conditions. In operational networks this would be uncommon and one would expect further message loss due to noise and other environmental effects. Our future work will repeat the experiments reported here but in the presence of noise. We expect that a black hole attack will be more detrimental in the presence of noise. One packet arrived at any of the 4 sinks provide 100% throughput. However, the effect of noise is most damaging under this circumstance. Also, echo, echo back and cluster key setup messages may be lost; this will reduce the number of legitimate neighbours and eventually the data throughput at the base station.

6. REFERENCES

[1] T.R. Andel and A.Yasinsac. Automated evaluation of secure route discovery in MANET protocols. In K. Havelund, R. Majumdar, and J. Palsberg, editors, *Proceedings of 15th International SPIN Workshop on Model Checking Software (SPIN 2008), Los Angeles, CA, USA*, volume 5156 of *Lecture Notes in Computer Science*, pages 26–41. Springer, 2008.

[2] J. Deng, R. Han, and S. Mishra. The performance evaluation of intrusion-tolerant routing in wireless sensor networks. In *IEEE 2nd International Workshop on Information Processing in Sensor Networks (IPSN'03), Palo Alto, CA, USA*, pages 349–364, 2003.

[3] J. Deng, R. Han, and S. Mishra. INSENS: Intrusion-tolerant routing for wireless sensor networks. In *Elsevier Journal on Computer Communications, Special Issue on Dependable Wireless Sensor Networks*, volume 29, pages 216–230, 2005.

[4] Y. Hanna, H. Rajan, and W. Zhang. Slede: a domain-specific verification framework for sensor network security protocol implementations. In *Proceedings of the first ACM conference on Wireless network security (WISEC '08), Alexandria, VA, USA*, pages 109–118, 2008.

[5] K. Saghar, W. Henderson, and D. Kendall. Formal modelling and analysis of routing protocol security in wireless sensor networks. In *PGNET '09*, pages 73–78, 2009.

[6] K. Saghar, W. Henderson, D. Kendall, and A. Bouridane. Formal modelling of a robustwireless sensor network routing protocol. In *NASA/ESA Conference on Adaptive Hardware and Systems (AHS-2010)*, 2010.

[7] K. Saghar, W. Henderson, D. Kendall, and A. Bouridane. Formal modelling of a robustwireless sensor network routing protocol. In *IEEE, IET International Symposium on COMMUNICATION SYSTEMS, NETWORKS AND DIGITAL SIGNAL PROCESSING NASA/ESA(CSNDSP 2010)*, 2010.

[8] L. Tobarra, D. Cazorla, and F. Cuartero. Formal analysis of sensor network encryption protocol (snep). In *IEEE Internatonal Conference on Mobile Adhoc and Sensor Systems (MASS 2007), Piscataway, NJ, USA*, pages 767–772, Pisa (Italy), 2007.

[9] L. Tobarra, D. Cazorla, F. Cuartero, G. Diaz, and E. Cambronero. Model checking wireless sensor network security protocols: Tinysec + leap. In *Proceedings of the First IFIP International Conference on Wireless Sensor and Actor Networks (WSAN'07)*, pages 95–106. IFIP Main Series, Springer, 2007.