In-Field Attack Proof of Injected False Data in Sensor Networks

Zheng Wang
Computer Network Information Center, Chinese Academy of Sciences, Beijing, China
Graduate University of Chinese Academy of Scienses, Beijing, China
Email: wangzheng@cnnic.cn

Xiaodong Lee[1], Xinchang Zhang[1,2] and Baoping Yan[1]
Computer Network Information Center, Chinese Academy of Sciences, Beijing, China[1]
Graduate University of Chinese Academy of Scienses, Beijing, China[2]
Email: {lee, zhangxinchang}@cnnic.cn, ybp@cnic.cn

***Abstract*—In a large-scale sensor network individual sensors can be compromised to inject bogus sensing reports. While SEF can filter out the outfield false reports, it is incapable of detecting the in-field compromised nodes, which may collect sufficient number of keyed message authentication codes (MAC). An in-field attack proof mechanism is presented in this paper. The MAC delivery mechanism makes the MACs follow the direction of increasing signal strength, and the skipping out mechanism helps the MACs walk out of the compromised nodes. As the report is forwarded, each node along the way verifies the correctness of the MACs probabilistically and drops those with invalid MACs. As the in-field compromised node is prevented from gathering enough MACs, the report generated by it can be detected and dropped en-route. Analysis and simulation show that IAP can drop bogus reports injected by an in-field compromised node in many cases.**

***Index Terms*—Compromised nodes, in-field attack, false data injection, wireless sensor network.**

I. INTRODUCTION

Wireless sensor networks are expected to interact with the physical world at an unprecedented level to enable various new applications. However, a large-scale sensor network may be deployed in a potentially adverse or even hostile environment and potential threats can range from accidental node failures to intentional tampering. Due to their relatively small sizes and unattended operations, sensor nodes have a high risk of being captured and compromised. False sensing reports can be injected through compromised nodes, which can lead to not only false alarms but also the depletion of limited energy resource in a battery powered network. Although several recent research efforts [1]–[3] have proposed mechanisms to enable node and message authentication in sensor networks, those proposed solutions can only prevent false reports injection by outside attackers. They are rendered ineffective when any single node is compromised (Fig. 1).

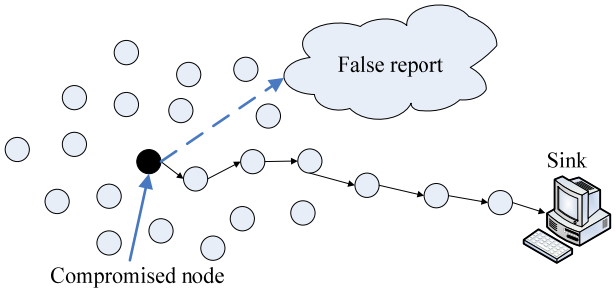

Figure 1. False report of compromised node.

To combat false reports injected by compromised nodes, one must have means to detect such false reports. However, developing such a detection mechanism represents a great research challenge. On the one hand, the computation and storage constraints of small sensor nodes make asymmetric cryptography based mechanisms, such as the one described in [4] [5], infeasible. On the other hand, straightforward usage of symmetric keys is infeasible because once a node is compromised, all the shared security information stored in that node can be used by an attacker. The compromised node can successfully authenticate bogus reports to a neighbor, which has no way to differentiate such false reports from legitimate ones.

As the first effort that addresses false report detection problems in the presence of compromised sensor nodes, [6] present a statistical en-route filtering (SEF) mechanism to detect and drop false reports during the forwarding process. SEF exploits the network scale to filter out false reports through collective decision-making by multiple detecting nodes and collective false detection by multiple forwarding nodes. Although SEF performs well for outfield compromised nodes, it is unable to filter out the false data generated by the in-field compromised nodes. The in-field compromised nodes can utilize their location to collect enough MACs for the en-route verification.

Supported by the Knowledge Innovation Program of the Chinese Academy of Sciences (No. O714011601)

In this paper, we present an in-field attack proof (IAP) mechanism. IAP exploits the sheer scale and dense deployment of large sensor networks and the shape of signal strength field formed by detecting nodes. To prevent any in-field compromised node from breaking down the entire system, IAP carefully designs the MAC routing mechanism. The MAC delivery mechanism makes the MACs follow the direction of increasing signal strength, and the skipping out mechanism helps the MACs walk out of the compromised nodes. As the report is forwarded, each node along the way verifies the correctness of the MACs probabilistically and drops those with invalid MACs. As the in-field compromised node is prevented from gathering enough MACs, the report generated by it can be detected and dropped en-route.

The rest of the paper is organized as follows. Sections II and III present the model of IAP and the design of SEF mechanism in GRAB. Section IV discusses the in-field attack for SEF. Section V presents the IAP mechanism. Section VI discusses the parameter setting and evaluates the design through simulations. Section VII presents related work in this area. Section VIII concludes the paper.

II. System models and assumptions

A. Sensor network model

We consider a sensor network composed of a large number of small sensor nodes. We further assumes that the sensor nodes are deployed in high density, so that a stimulus (e.g., a tank) can be detected by multiple sensors. Each of the detecting sensors reports its sensed signal density and one of them is elected as the center-of-stimulus (CoS) node. The CoS collects and summarizes all the received detection results, and produces a synthesized report on behalf of the group. The report is then forwarded toward the sink, potentially traversing a large number of hops (e.g., tens or more). Due to cost constraints we assume that each sensor node is not equipped with tamper-resistant hardware.1 However, dense deployment enables cross-verification of a reported event among multiple sensors even in the presence of one or more compromised nodes. IAP design harnesses the advantage of large-scale. Rather than relying on a small number of powerful and expensive sensors, IAP utilizes large numbers of small sensors for reliable sensing and reporting.

B. Threat model

We assume that the attacker may know the basic approaches of the deployed security mechanisms, and may be able to either compromise a node through the radio communication channel, or even physically capture a node to obtain the security information installed in the node. However, we assume that attackers cannot subvert the data collection unit, i.e., the sink, because the protection at the sink is powerful enough to defeat such subversion efforts. Once compromised, a node can be used to inject false reports into the sensor network. Node and message authentication mechanisms [1]–[3] prevent naive impersonation of a sensor node. However, they cannot block false injection of sensing reports by compromised nodes. Besides false data injection, a compromised sensor node can launch various other attacks. It can stall the generation of reports for real events, block legitimate reports from passing through it (which we call false negative attacks), or record and replay old reports, etc. As the first effort in tackling the threats from compromised components, this paper focuses on the detection of false event reports, which we call false positives attacks, injected by compromised nodes. We plan to address other attacks in subsequent efforts.

One common type of attack is targeted at message authenticity and integrity. For example, if the sender and the receiver are not within the transmission range of each other, an intruder on the path connecting them can modify passby messages or inject false messages. It appears to be a solution that the sender and the receiver share a secret key, and the shared key is used by the sender to generate message authentication code for any outgoing message, and by the receivers to verify the authenticity and integrity of any incoming message. If a message is tampered en route, it will be detected by the receiver. This method however is not effective due to the following reasons: First of all, it cannot authenticate messages that are multicast because, if one of the receivers is compromised, the intruder can use the secret key held by the compromised receiver to fake MACs for messages modified or injected by it itself to cheat other receivers. Secondly, the method only allows end-to-end message authentication while en-route forwarding nodes cannot authenticate passby messages; as a result, the intruder may launch denial-of-service attacks by repeatedly modifying messages or injecting false messages to deplete the communication resources of intermediate forwarding nodes.

Besides false data injection, a compromised sensor node can launch various other attacks. It can stall the generation of reports for real events, block legitimate reports from passing through it (which we call false negative attacks), or record and replay old reports, etc. As the first effort in tackling the threats from compromised components, this paper focuses on the detection of false event reports, which we call false positives attacks, injected by compromised nodes.

III. SEF mechanism in GRAB

A. GRAdient broadcast

GRAdient Broadcast [7] (GRAB) is designed specifically for robust data delivery in face of unreliable nodes and fallible wireless links. The election of a source in GRAB follows the following mechanism. GRAB wants only CoS to generate the report since it would be a waste of resources if every node detecting the stimulus sends a report. The stimulus creates a field of sensing signal strength, the “shape” of which is similar to that of the cost field. Each node broadcasts a message indicating its signal strength (with some random delay to avoid

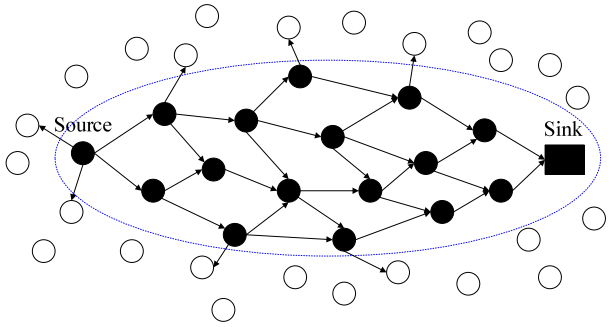

Figure 2. The forwarding mesh of GAB.

collision). A node rebroadcasts its signal strength whenever it hears a neighbor's message with a weaker signal, but stops broadcasting when it hears a stronger one. This way, messages roll towards the center of the signal strength field. Finally the node with the strongest signal or CoS generates a report (Fig. 2).

B. En-route filtering mechanism

In SEF [6], the sink maintains a global key pool. Each sensor stores a small number of keys that are drawn in a randomized fashion from the global key pool before deployment. Whenever a stimulus appears in the sensor field, multiple surrounding nodes can detect the event and CoS is elected to generate the event report. Each detecting sensor endorses the report by producing a keyed MAC using one of its stored keys. CoS collects the MACs and attaches them to the report. This set of multiple MACs acts as the proof that a report is legitimate. A report with insufficient number of MACs will not be forwarded. The key assignment ensures that each node can generate only partial proof for a report. Only by the joint efforts of multiple detecting nodes can the complete proof be produced. A single compromised node has to forge MACs to assemble a seemingly complete proof in order for the forged data report to be forwarded.

Because nodes share common keys with certain probabilities, when the report with forged MACs is forwarded by intermediate nodes, the nodes can verify the correctness of the MACs probabilistically, thus detecting and dropping false ones en-route.

The sink serves as the final goal-keeper for the system. When it receives event reports, the sink can verify all the MACs carried in the report because it has complete knowledge of the global key pool. False reports with incorrect MACs that sneak through en-route filtering will then be detected.

C. SEF mechanism in GRAB

As proposed in SEF, keyed MACs generated by detecting sensors are utilized to verify the correct CoS and filter the false data. Thus the election of a source in GRAB should be modified by SEF as follows. The sink maintains a global key pool. Each sensor stores a small number of keys that are drawn in a randomized fashion from the global key pool before deployment. Whenever a stimulus appears in the sensor field, the stimulus creates a field of sensing signal strength, and then every node rebroadcasts its signal strength. whenever a node hears its

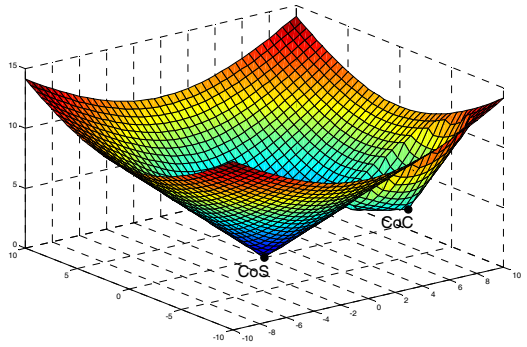

Figure 3. The signal strength field.

neighbor's reporting with a stronger signal, the sensor endorses its report by producing a keyed MAC using one of its stored keys and attaches all the MACs including its own and those it received to its message. Then the sensor delivers its message to the neighbor reporting stronger signal strength. If a node never hears a stronger reporting from its neighbors, it seems to be the CoS node given that there is no attackers. So it does not need to deliver its message and all it need to do is to collect all the message or MACs from nodes in the field of sensing signal strength. Note that the process of message forwarding needs to last for a while, as it would take some time for the nodes to collect and deliver as many as possible MACs. During the convergence of MACs' delivery, the node combines the MACs contained in all the messages it received and removes the reduplicate ones to save network resources. MACs travel in the field of sensing signal strength like water flows down to the bottom of a funnel: they follow the direction of decreasing signal strength to reach the bottom of the field, which is the CoS node. Theoretically the CoS node should gather all the MACs and no other nodes can own even a small part of the total MACs.

IV. IN-FIELD ATTACK FOR SEF

SEF assumes that the compromised node is outside of the field of sensing signal strength, so only a relative small number, if not none, of surrounding nodes can deliver their MACs of report to the compromised node following the mechanism of CoS election described above. These surrounding nodes that elect the compromised node may also be compromised by the attackers, this group of compromised nodes are controlled or captured by the attackers which are intended to accumulate as many MACs as possible to support one compromised node. However, there are no other nodes which will elect or deliver their MACs to the compromised node for they do not detect the signal strength. So the report generated by the compromised node cannot collect sufficient number of MACs to be treated as the proof that the report is legitimate. Thus in the outfield situation SEF can be considered effective and trustworthy.

However, SEF does not work well when the compromised node is inside of the field of sensing signal

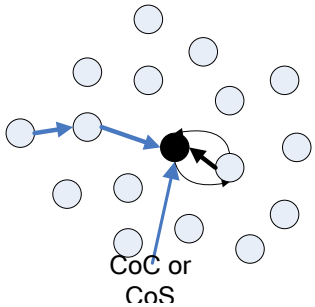

Figure 4. MAC's routing without path list.

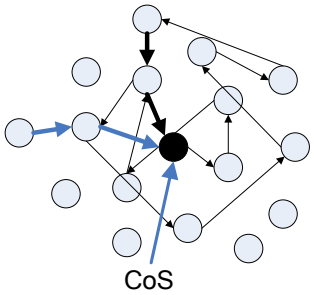

Figure 5. MAC's routing around CoS

strength. As the SEF mechanism in GRAB described above shows, when the surrounding nodes of the compromised one hear its forged reporting with a stronger signal, they would send their messages to the compromised node. And the compromised node, cheated by the injected false data, would never deliver its message to any one. Because the surrounding nodes themselves may carry many MACs they received in their messages, the compromised node can collect a sufficient number of MACs so that there is no need for it to forge MACs. Then the MAC verifying mechanism by SEF in GRAB proves to be useless. The situation seems to be even more severe considering a group of compromised nodes may coalesce to attract nodes in a large area. These compromise nodes seek to elect the center of them to be forge CoS, which we call the center of compromised nodes (CoC). When there are compromised nodes, the field of sensing signal strength is much like a funnel with two bottoms as shown in Fig. 3: one for CoS, the other for CoC. So a comparably great mount of water flows down to the bottom shaped by the compromised nodes just like it moves to the CoS's bottom. The bottom for the compromised nodes may be carefully constructed by the attacker in order to looks like a real one. For example, the attacker may utilize many other compromised nodes around CoC to make a funnel shape. Thus many MACs follow the direction of increasing signal strength to reach the bottom of the field, which is the compromised node but not CoS.

IV. IAP MECHANISM DESIGN

A. IAP mechanism

IAP consists of two main mechanisms: 1) the MAC delivery mechanism makes the MACs follow the direction of increasing signal strength; 2) The skipping out mechanism helps the MACs walk out of the compromised nodes.

The process of IAP goes through there stages: 1) MAC delivery 2) skipping out 3) MAC delivery again. The first stage aims to find the possible CoS; the second stage is to test the reality of the CoS found in the first stage and escape from the counterfeit one; the last stage aims to find the real CoS.

The MAC delivery mechanism modifies the SEF mechanism in GRAB described above by adding one-hop further look when a node decides how to delivery its message. When a node hears a neighbor's message with a stronger signal, it requests a reply from the neighbor reporting whether the neighbor hears a stronger one. The aim of this request is to decide whether the neighbor can be regarded as the possible CoS. If the neighbor reports that it hears a stronger message, which means it can not be CoS, the MAC delivery process goes on just as the SEF mechanism in GRAB. This either indicates that the MACs are being forwarded in the correct direction, or they have not encountered the forged CoS. If the neighbor answers that it hears no stronger message, which means it claims to be the CoS, the MAC delivery process pauses temporarily, and the skipping out process begins.

As a single or a group of nodes may be compromised by the attacker, the signal strength they reported is not creditable. The skipping out process aims to make MACs get out of the local area that may be "polluted" by the false data, and let the "pure" outer region of the field of signal strength to direct the MAC delivery. When a node receive a reply from its neighbor indicating that it hears no stronger message which means that the neighbor can be the possible CoS, it send its ordinary signal message to the neighbor together with a commanding message which informs the neighbor that the skipping out mechanism starts. Then the neighbor node forwards the signal message it received to its neighbor with the strongest signal strength except its recent backward node since the start of the skipping out process. At every step of the message forwarding, the node adds itself to the list of the recent backward nodes and send the signal message with this list (which we call path list for convenience). This process may repeat several times or the original message at the start of the skipping out mechanism may be forwarded by several steps. The purpose of this forwarding design is to maintain the direction of increasing signal strength while avoiding the path circle.

Note that without the path list, the forwarding may fall into local stronger area and can not move on. A simple case of path circle shows in Fig. 4. In Fig. 4, the block node is CoC or CoS and the other nodes are ordinary ones around it. The wide arrows with shallow color denote the first stage of MAC delivery and the wide arrows with black color denote the second stage of MAC delivery. The narrow arrows denote the stage of skipping out. If two nodes (CoC or CoS and a node near it) are with relatively stronger signal strength, the message would be propagated back and forth between the two nodes forever. To prevent the message from getting into the path cycle, we maintain the list of the recent backward node in the

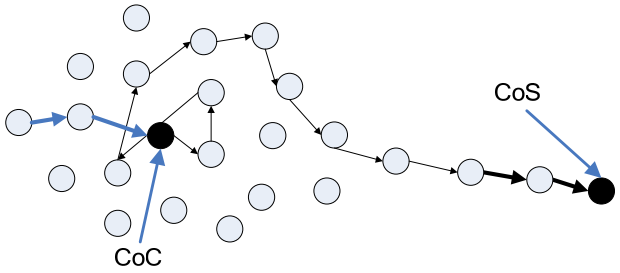

Figure 6. MAC's routing around CoC.

message and force the forwarding to explore new nodes continuously.

There are two cases that we need discuss here. If the CoS found in the first stage is the real one, the skipping out process simply makes the MAC travel in the surrounding field of CoS due to the field shape formed by the CoS. Fig. 5 shows the MAC's routing around CoS (the denotation of the symbols is the same as Fig. 4). Due to the descending signal strength from CoS, MACs are "glued" by CoS in the approximal space in the stage of skipping out. Thus when the second MAC delivery comes, MACs are certain to be drawn back to CoS.

While as for the forged CoS or CoC, the skipping out process is likely to move to the ordinary node which lies in the field of the real CoS. Fig. 6 shows the MAC's routing around CoC (the denotation of the symbols is the same as Fig. 4). Within a number of hops of skipping out, if not one (due to the quite limited amount of compromised nodes), MACs are routed to outer space of compromised nodes. Then in the "pure" region the second MAC delivery can successful lead the MACs to CoS.

Note that the message forwarding may be retained in the compromised nodes at the starting few steps, but as more compromised nodes are consumed during the forwarding, the MACs are more likely to move to the ordinary nodes. Once this happens, the skipping out process is much like the delivery process delivery process except avoiding moving to the list of the recent backward node. And so finally MACs move in the direction of increasing signal strength to an ordinary node.

When the skipping out process ends, the MAC delivery process starts again. As the starting node is in the field of the real CoS, the MAC delivery mechanism described above can make MACs head for the real CoS.

IAP guarantees compromised node's insufficient MACs, thus the false report generated by it can be statistically dropped en-route by the en-route filtering mechanism described in section III.B.

B. Design tradeoff

While IAP can be expected to work well in most cases, we can not neglect the specific case, though fairly scares, which undermines the effect of IAP.

One such case is that what is if the compromised nodes are quite near CoS? CoC can attract more MACs in the first stage of MAC delivery, even almost equal to the number by CoS. What is worse is that the skipping out stage only makes the MACs gathered by CoS to skip to the compromised area with high possibility. The extreme situation is that the whole MACs fall into either area (CoS or CoC) at random. It looks as if the two centers are bond together and we can not distinguish them easily. Since we utilize the signal strength information in IAP, we can also find the solution in the correlation of signal strength field. One way is sensing the signal strength of the nearby nodes when reaching the possible CoS in the first MAC delivery stage as well as when passing the routing nodes in the skipping out stage. The signal strength difference between nodes can be estimated by the energy decreasing model in the space of wireless sensor networks. If the current node is inconsistent with nearby nodes in the signal strength, it can be regard as the compromised one. However, this approach will consume much more energy which seems too costly in many scenarios. Actually the problem is not so seriously as it looks like. The aim of the attacker is to report to the sink the false position departing from the true one as far as possible. A minor departure from CoS means little benefit to the attacker. Suppose a enemy tank is targeted by sensor network for military monitoring, though with a little position error caused by the compromised nodes, missiles can still be navigated to the tank and destroy it, only if the tank lies in the bombing area.

Another case is that when the sensor is scattered quite sparsely can IAP still work? Unfortunately since IAP design harnesses and rely highly on the advantage of large-scale, we can not expect IAP to work well in such case. As for the underlying mechanism of IAP, the success ratio of GRAB is low for low sensor density [7]. The reason is that there are not enough nearer neighbors when node density is low. Thus the forwarding stops where there are not enough nearer neighbors to combat node failures and packet losses. However, the success ratio remains high above 90% for all the high densities. This makes sense in that high density produces high accuracy in positioning.

As for the design tradeoff considerations, energy consumption is the main cost of detecting near-field compromised nodes, and if we do not need such high differentiating ability, we can save that energy while still maintaining required accuracy. High enough sensor density is the necessity for IAP, and in low densities the performance can be dramatically enhanced by increasing the density while this enhancement is not so apparent. We will further discuss this problem and show some results in section VI.

VI. PERFORMANCE EVALUATION

A. Parameter selection

In this section we discuss the impact of parameter choices on IAP effectiveness.

1) The number of hops of skipping out: The main impact of this parameter H which is on skipping out efficiency. H must be large enough to enable skipping out the compromised field. Because too few hops may not let MACs go through all of the compromised nodes. But it should not be too big. With a too big number of hops, the energy of the nodes is unnecessarily consumed and more

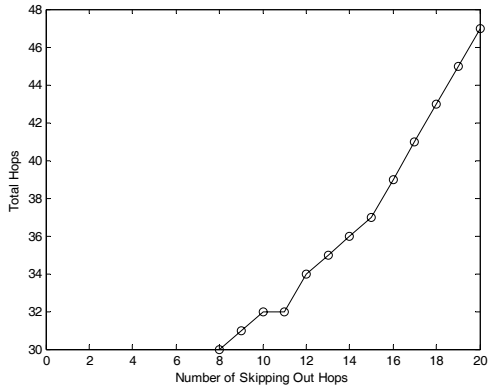

Figure 7. Total hops for different number of skipping out hops.

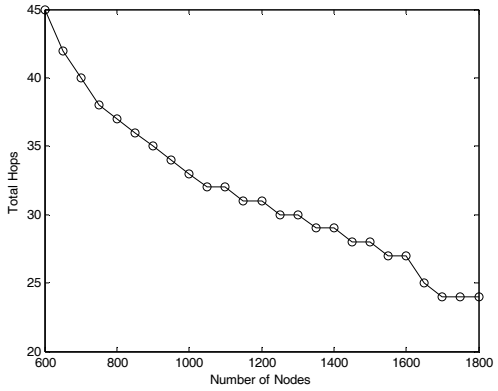

Figure 8. Total hops for different number of skipping out hops.

time is taken to complete the MAC delivery. H should be decided based on the number of compromised nodes N. We propose that H should be comparable to N in most cases.

2) Deployment density: Another factor we must consider is the node deployment density ρ. Because the MAC delivery mechanism and the skipping out mechanism utilize the high density of sensor nodes, ρ should not be too small. In addition since we require MACs from distinct categories for each legitimate report, the number of detecting nodes for the same stimulus should be large enough to possess keys from at least partitions.

3) Sensing range of nodes: Sensing range of nodes S also impact on IAP. Large range is usually preferred to allow for better constraint on the MACs around CoS. Because the MACs can take fewer hops to reach CoS in the second stage of MAC delivery.

B. Simulation results

In this section we evaluate the performance of IAP through simulations. The maximum transmission range of a node is 10 meters, each node can adjusts its transmitting power to reach a given range. We simulated our test scenarios under both the two ray ground and the free space signal propagation models. The transmission (receiving) time for a packet is 10 ms.

In most scenarios, we use a field size of $150\times150m^2$ where 1200 nodes are uniformly distributed. One sink and one source sit in opposite corners of the field. The source generates a report packet every 10 seconds. In each run 100 reports are generated.

We study how the number of hops of skipping out affects IAP. We keep the other parameters the same and the number of compromised nodes C as 10, while varying H from 1 to 20. We use the total hops of the MAC routing T as the evaluation metric as small one of it indicates less transmission time and energy consumption. As Fig. 7 shows, for H less than 8, the MACs never reach CoS, so T can be seen as infinity. For H larger than 8, T changes with H, from about 30 hops to about 47 hops. This demonstrates that 8 is the optimal option of H in this case.

To find how the density of nodes can affect IAP, we keep the field size 150 × 150 m^2, while varying the number of nodes from 600 to 1800 (keeping C=10, H=10). Fig. 8 shows how the total hops of the MAC routing changes over different node numbers.

To study the impact of sensing range, we keep the other parameters the same and vary sensing range from 5 to 20. Fig. 9 shows how the total hops of the MAC routing changes over different sensing ranges.

VII. RELATED WORK

In this section, we present some relevant research pertaining to false data rejection and secure protocols.

To defend against such attacks, the digital signature-based technique can be used to authenticate and filter false messages. However, this technique has high overhead both in terms of computation and bandwidth [5], which makes it unsuitable for sensor networks [6]. Therefore, researchers proposed to adopt symmetric cryptographic techniques. Ye et al [6] propose a statistical en-route filtering scheme (SEF), which allows both BS and en-route nodes to detect false data with a certain probability. Zhu et al [8] propose an Interleaved Hop-by-Hop Authentication Scheme (IHHAS) where pairwise keys are established between nodes t+1 hops away and up to t compromised nodes can be tolerated. Yang et al. [9] present a commutative cipher based en-route filtering scheme (CCEF) which is based on public-key algorithms that have been reported not suitable for sensor networks due to limited resource capacity of sensor nodes [12]. Yu et al [10] present a dynamic en-route filtering scheme for filtering false data injection; alleviating the constraint of fixed path requirement between BS and CH in [8], [9]; thus, making the scheme better suited to deal with dynamic topology of sensor networks. Zhang et al. [13] present the interleaved authentication for filtering false data in multipath routing based sensor networks. Przydatek et al [11] present SIA for secure aggregation in sensor networks. It focuses on reducing trust in BS, when queried by a trusted outside user and gives schemes to compute a few aggregation primitives. Utilizing an one-way key chain and delayed disclosure of keys, the TESLA schemes [14] and its variants can achieve message authenticity in the presence of a large number of node compromises. However, these schemes require synchronization among nodes. They introduce delay in

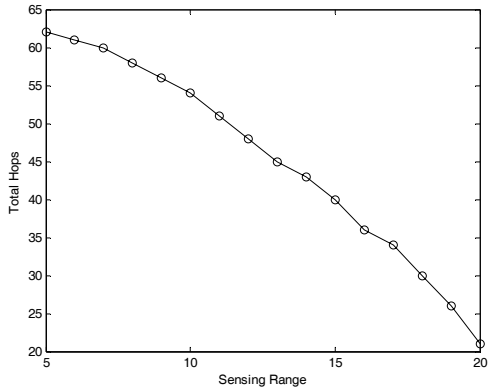

Figure 9. Total hops for different number of skipping out hops.

message authentication and the delay increases as the network scales up. Moreover, they repel the adoption of asynchronous communication [15]. To identify the compromised nodes, each node can use the watchdog mechanism [16] to monitor its neighbors and identify the compromised nodes when observing misbehaviors. The collaborative intruder identification scheme proposed by Wang et al. [17] can also be used to improve the accuracy.

Novelty of our work: There is significant difference between past research and our work. In general, past research has focused on filtering outfield false data, Similarly, false data rejection protocols involve accepting or rejecting single values which are proven equal (with some tolerance) or not equal to each other. As discussed earlier, this leads to in-field attack insecurity. Thus, we focus on solving a novel problem: how to resolve an in-field phenomenon by utilizing large scale sensor network. In general, it is difficult to distinguish between real and false data if complicated key manage mechanism is not utilized. Our another contribution is that instead of focusing finding the secure cryptology, we make full use of the simple formation of signal strength field. In our scheme, the sensor nodes also collectively authenticating the signal strength field besides authenticating the MACs.

VIII. CONCLUSION

Large-scale sensor networks may be deployed in a potentially adverse or even hostile environment. Due to the unattended operations of the network and the relatively small sizes of the sensors, sensor nodes may have a high risk of being captured and compromised. In this paper, we focused on detecting false sensing reports that can be injected by compromised nodes. IAP design harnesses the advantage of large-scale by leverage the signal strength field to lead the MACs to escape from the compromised field and reach CoS finally. Our analysis and simulations show the good performance of IAP though influenced by several parameters. IAP represents the first step toward building resilient sensor networks that can withstand in-field compromised nodes.

ACKNOWLEDGMENT

The authors wish to thank all staff of China Internet Network Information Center (CNNIC) Labs. This work was supported in part by a grant from the Knowledge Innovation Program of the Chinese Academy of Sciences.

REFERENCES

[1] Wensheng Zhang, Subramanian N., and Guiling Wang, "Lightweight and Compromise-Resilient Message Authentication in Sensor Networks", *Proc. of the IEEE INFOCOM 2008*, IEEE Communication Society, Phoenix, 2008, pp.1418-1426.

[2] Chan H, Perrig A, "PIKE: Peer intermediaries for key establishment in sensor networks", *Proc. of the IEEE INFOCOM 2005*, IEEE Communication Society, Piscataway, 2005, pp.524-535.

[3] Younis M, Ghumman K, and Eltoweissy M, "Location-Aware combinatorial key management scheme for clustered sensor networks", *IEEE Trans. on Parallel and Distribution System*, 2006, 17(8): pp.865-882.

[4] Eltoweissy M, Moharrum M, and Mukkamala R, "Dynamic key management in sensor networks", *IEEE Communications Magazine*, 2006, 44(4): pp.122-130.

[5] Zhang YC, Liu W, Lou WJ, Fang YG, "Location-Based compromise-tolerant security mechanisms for wireless sensor networks", *IEEE Journal on Selected Areas in Communications*, 2006, 24(2): pp.247-260.

[6] Ye F, Luo H, Lu S, "Statistical En-route Detection and Filtering of Injected False Data in Sensor Networks", *IEEE Journal on Selected Areas in Communications*, 2005, 23 (4): pp.839-850.

[7] Ye F, Zhong G, Lu S, "GRAdient Broadcast: A Robust Data Delivery Protocol for Large Scale Senor Networks", *ACM Wireless Networks*, 2005, 11(3): pp.285-298

[8] S. Zhu, S. Setia, S. Jajodia, and P. Ning, "An interleaved hop-by-hop authentication scheme for filtering false data injection in sensor networks," *Proc. Of the IEEE SSP 2004*. IEEE Computer Society Press, 2004: pp.259-271.

[9] H. Yang and S. Lu, "Commutative cipher based en-route filtering in wireless sensor networks," *Proc. Of the IEEE VTC 2004*. IEEE Computer Society Press, 2004: pp.129-141.

[10] Z. Yu and Y. Guan, "A dynamic en-route scheme for filtering false data injection in wireless sensor networks," *Proc. Of the IEEE INFOCOM 2006*. IEEE Computer Society Press, 2006: pp.59-71.

[11] B. Przydatek, D. Song, and A. Perrig, "SIA: Secure information aggregation in sensor networks," *Proc. Of the ACM SenSys 2003*. ACM Press, 2003: pp.87– 92.

[12] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," *Proc. Of the ACM CCS 2002*. ACM Press, 2002: pp.41 – 47.

[13] Y. Zhang, J. Yang, and H. Vu, "Interleaved authentication for filtering false reports in multipath routing based sensor networks," *Proc. Of IEEE IPDPS 2006*. New York: IEEE Computer Society Press, 2006: pp.23-29.

[14] A. Perrig, R. Canetti, J. Tygar, and D. Song, "Efficient Authentication and Signing of Multicast Streams over Lossy Channels," *Proc. of the IEEE Symposium on Security and Privacy 2000*. Los Alamitos: IEEE Computer Society Press, 2000: pp.56-73.

[15] S. Bhattacharya, H. Kim, S. Prabh, and T. Abdelzaher, "Energy-Conserving Data Placement and Asynchronous Multicast in Wireless Sensor Networks," *Proc. of the ACM MobiSys 2003*. New York: ACM Press, 2003. 1(2): pp.178-203.

[16] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," *Proc. of the ACM MobiCom 2000*. New York: ACM Press, 2000. pp.255-265.
[17] G. Wang, W. Zhang, G. Cao, and T. La Porta, "On Supporting Distributed Collaboration in Sensor networks," *Proc. of the IEEE Military Communications Conference (MILCOM) 2003*, Boston: IEEE Press, 2003. pp.752-757.

Zheng Wang is born in ShanDong province, China in 1979. He is a Ph. D. candidate at Computer Network Information Center, Chinese Academy of Sciences, China. He received his M.S. and B.S. degrees both in Electrical Engineering from Institute of Acoustics, Chinese Academy of Sciences in 2006 and from University of Science and Technology of China in 2003 respectively. His research interests include ad-hoc and sensor networks, peer-to-peer systems, network measurements, and multicasting.

Xiaodong Lee is born in ShanDong province, China in 1976. He got his Bachelor in the Computer Science Department of Shandong University (SDU), and then, Master in CNIC of CAS , where he continued his doctoral research, and achieved my Ph.D. in the Institute of Computing Technology (ICT) of CAS in 2003. He is now an Associate Professor of Chinese Academy of Sciences(CAS), and the Vice President and Chief Technical Officer of China Internet Network Information Center(CNNIC). His interests focus on the application exchange technologies, e.g. PKI, DNS, ENUM, RFID and etc., He is also interested at following research area: network administration, information security, grid computing, NGI/NGN, ubiquitous computing.

Xinchang Zhang is born in ShanDong province, China in 1975. He received the B.S. degree from the Chongqing Jiaotong University, China, the M.S. degree from the Shandong University of Science and Technology, China, and is working toward the Ph.D. degree at Computer Network Information Center, Chinese Academy of Sciences. His research interests include network protocols and architectures and overlay networks.

Baoping Yan is born in ShanDong province, China in 1950. She is Professor, Chief Engineer, Supervisor of Ph.D. students of Computer Network Information Center, Chinese Academy of Sciences (CAS); Board Member, The Internet Society (ISOC); Director, Office of Informatization Leading Group for Chinese Academy of Sciences; Deputy Director, CODATA Chinese Committee; Deputy Director, Working Committee for Scientific Database of CAS. Her research interests include scientific data base, next generation network, network addressing and network measurements.