SBGR: A Simple Self-Protected Beaconless Geographic Routing for Wireless Sensor Networks

Rafael Marin-Perez, Pedro M. Ruiz
Dept. of Information and Communications Engineering
University of Murcia,
{rafael81,pedrom}@um.es

***Abstract*— In geographic routing a node forwards data packets to a neighbor which is closer to the destination than itself. However, most of the existing geographic routing protocols have not been designed to work effectively in scenarios with malicious nodes. Some protocols use cryptographic schemes, reputation schemes and other sorts of complex and costly (especially for a wireless sensor network) solutions to provide security to the routing protocols. Moreover, these schemes are not able to deal with attacks from legitimate nodes compromised (insider attacks). We analyze in detail the effects of insider attacks (Sybil and Sinkhole) in beaconless geographic routing protocols and propose a Self-Protected Beaconless Geographic Routing (SBGR) protocol. We show that by just enhancing the forwarding logic of our routing protocol to make additional transmissions when suspicious traffic is detected, we can deal with these insider attacks without the extra cost and overhead of deploying complex reputation systems. Our simulations show that SBGR outperforms existing solutions and achieves nearly a 100% packet delivery ratio with a very low additional overhead.**

I. Introduction

A Wireless Sensor Network (WSN) consists of a set of hundreds or thousands of battery-powered and lightweight devices equipped with sensor hardware to monitor the environment. To transmit sensed information, nodes act as routers using their wireless interface to forward the packets from the source to the destination.

Geographic Routing (GR) is one of the most efficient routing techniques for wireless sensor networks. GR is based on the location information of neighboring nodes to take forwarding decisions. Nodes forward packets to their neighbors located closer to the destination than themselves. GR assumes that localization systems exist to determinate geographic or virtual positions of nodes [1], [2]. To discover neighbor's positions, nodes use periodic transmissions of short packets also called beacons. Beacons cause severe problems in real scenarios: collisions, imprecision in neighborhood tables, useless waste of resources, etc. Therefore, beacon-less protocols such as IGF [3], BOSS [4], BLR [5], GeRaF [6], ALBA [7] and ROME [8] have been proposed for WSNs to overcome these disadvantages.

However, beaconless protocols have not been designed to work in unsafe environments where an attacker can exploit the shared wireless medium to severely affect communications [9], [10]. For instance, a sinkhole attacker acts as a neighbor taking part in the forwarding process to intercept and drop data packets. A sybil attacker can use multiple identities associated with different positions to pretend being the best relay for all forwarding operations happening within its radio range. Once the attacker gets selected as the next relay it can drop the packet.

To provide security in geographic routing, trust-management, location-verification and cryptographic mechanisms have been proposed. Trust management is based on neighbors' reputation to penalize the anomalous behavior of attackers. Location verification [11], [12] uses ultrasonic hardware to measure the distance between nodes to verify the reported location. Nodes using cryptographic mechanisms ([13], [14]) share symmetric keys to authenticate and encrypt the packets. However, these mechanisms require extra hardware and energy. In addition, cryptography is insufficient against insider-attackers being able to get private keys and compromise routing protocols [9]. Unlike previous solutions, we argue that by considering these issues in the design of the protocol, we can avoid those security problems without the extra cost of setting up complex reputation and cryptographic schemes.

We present a Self-Protected Beaconless Geographic Routing protocol (SBGR) for WSNs. SBGR is based on a simple beaconless protocol where nodes compete in a distributed way to forward the packets. This distributed forwarding is designed to prevent attackers intercepting and dropping packets. Nodes overhear the forwarding of their neighbors to detect malicious behaviors (e.g. receiving an packet from a node located outside its radio range). The way in which our protocol is designed makes it able to deal with different kind of attacks ranging from basic sinkhole attacks, to more elaborate sybil attacks where attackers may create fake identities with arbitrary locations. In addition, when attacks occur, nodes only need local information to autonomously retransmit packets toward the destination. Our simulations show that SBGR achieves almost a 100% delivery ratio with a lower control overhead than competing solutions.

The remainder of the paper is organized as follows. Section II gives an overview of existing secure routing solutions. Section III analyzes in detail the behavior of attackers in beaconless geographic routing. Section IV describes our proposal and the way it deal with insider attackers. Section V evaluates our proposal against the best-performing secure beaconless protocol in the literature. Finally, Section VI provides our final conclusions and future works.

II. Related work

In GR, nodes only need local topology information to take forwarding decisions. A node selects as the next-hop to forward the packets the neighbor that is located the closest to the destination. When there are no closer neighbors, a recovery scheme is applied to route around the perimeter of the so called void area.

Location information is a critical factor in GR. Attacks using false location information can compromise routing decisions. An attacker can simulate a false location that is closer to the destination than any candidate neighbor and drop all traffic. An attacker can inject false positions of its neighbors to generate routing loops or void areas.

Several location verification mechanisms have been proposed to prevent false information. Sastry et al.[15] provide a location verification using ultrasonic hardware to measure the distance between nodes. SeRLoc [11] is a range independent localization algorithm based on beacons transmitted from fixed nodes acting as reference points. Capkun et al. [16] present a range dependent positioning system based on distance bounding and verifiable multi-lateration. Zang et al. [17] assess the trusted location of nodes through triangulation and RF-based fingerprinting methods.

There are also existing solutions to provide authentication and encryption at the link-layer to routing protocols in WSNs. SPINS [13] and TinySec[14] use symmetric cryptography or hashing to maintain routing or discovering new routes.

Trust management is one of the most popular techniques to secure routing protocols in WSNs. The basic idea is overhearing the transmission of nodes and keep reputation information according their behaviors. Nodes penalize low reputations to select legitimate neighbors to forwards the packets. Boukerche and Li [18] propose a localized trust and reputation management that considering the system perspectives reduces the energy, bandwidth consumption and delay.

SIGF [19] is the unique secure routing proposal adapted to beaconless geographic routing. SIGF is a family of routing protocols in increasing of the complexity and security. SIGF-0 keeps no state and provides probabilistic defenses. SIGF-1 uses local history and trust management to protect against insider attacks. Finally, SIGF-2 uses information shared among neighbors to provide stronger security guarantees.

However, existing solutions do not adapt to the stringent resources of sensor nodes. These mechanisms require specific hardware, maintaining reputation tables and complex cryptographic operations. Moreover, cryptography is insufficient to provide a reasonable protection against insider attacks [9]. The reason is that an insider attacker has valid cryptographic keys that allow it to participate in the network and send valid routing and data packets. So, to get protected from these attacks routing protocols need to perform additional operations.

In the next section, we analyze insider attacks and how they affect the performance of beaconless geographic routing.

III. Insider Attacks against Beaconless Geographic Routing

Before we get into details about the security of beaconless geographic routing protocols, we give below some background about beaconless geographic routing and the two general forwarding schemes used by these solutions.

A. Data Forwarding Schemes in Beaconless GR

Beacon-based geographic routing protocols send periodic 1-hop hello messages which are used by nodes to know their neighbors and their positions. To avoid the overhead, contention, etc. caused by beacons, beaconless geographic routing protocols use a reactive neighborhood discovery. That is, the current node routing the data packet broadcasts a message and neighbors answer with their positions.

To avoid too much overhead, responses are usually ordered according to a delay function and the first response cancels other responses. So, if a neighbor is better according to some routing metric than others it waits less time before answering, and other neighbors can cancel their responses. For instance, if the routing metric is distance to destination, the neighbor which provides more progress towards the destination answers first.

Existing beaconless routing protocols differ on small details regarding how the operation described above is carried out. For instance, some protocols broadcast a control message to discover neighbors, other protocols broadcast the data packet first, different protocols use different delay functions, etc.

We can group existing solutions into two different approaches of beaconless forwarding schemes: three-way handshake (i.e. IGF) and distributed forwarding (i.e. BLR). Three-way handshake consists of the exchange of three messages (query-response-select) between the current sender and its neighbors. The current sender broadcasts a query message to discover its neighbors that set a delay time according their positions. After waiting for its computed delay, a node reports back its position and identifier (response message). As we said before, the best node waits less time, so its answer cancels the responses from other neighbors. Finally, the sender explicitly sends the data packet to the selected neighbor.

Distributed forwarding uses an unique broadcast message to discover and forward the data packet. Neighbors receiving the data packet use a delay time to compete in a distributed way to become the next hop. Finally, the neighbor located the closest to the destination re-broadcasts first the data packet cancelling the rest of candidates. Note that this also initiates again the forwarding process.

Several works [9] study insider attacks against geographic routing protocols in WSNs. The goal of insider attacks is to reduce the performance of routing protocols in terms of delivery ratio, number of transmissions, etc. Insider attacks can be classified into three categories according to how they affect beaconless protocols.

1) Attacks that compromise routing information used for nodes in the forwarding such as State corruption (i.e. disseminate erroneous routing tables), HELLO Flood (i.e. exchange beacons with false positions among neighbors) and Wormholes (i.e. simulate tunnels between two distant nodes). These attacks to routing do not affect beaconless protocols because they do not maintain any routing information. Beaconless GR protocols perform

a per-packet next hop selection which does not rely on previous information.

2) Denial-of-service attacks generate useless traffic to overload the nodes and jeopardize the overall performance. The goal of this attack is to waste the stringent resources of nodes in terms of energy and bandwidth. Denial-of-service attackers record and replay legitimate messages to reduce the performance of beaconless protocols. These attackers replace the identity of the sender and generate unlimited duplicate packets. To avoid denial-of-service, beaconless protocols require sophisticated cryptographic mechanisms to only forward data packets for which the identity of the sender can be validated.
3) Attackers trying to intercept all traffic in their coverage area to suppress it (i.e. Sinkhole and Sybil). They can act as legitimate neighbors taking part in the routing process in order to become the next forwarder. These attacks are the worst enemy for beaconless geographic routing protocols and we analyzed them in detail below.

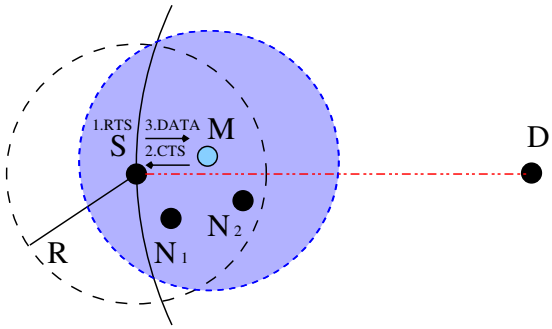
Sinkhole and sybil attacks exploit the forwarding process of beaconless protocols by pretending to be the best relay. These means responding before other neighbors and pretending to be located closer to the destination than any other neighbor. When a sinkhole attacker manages to gets the data packet it just drops it. Sybil attacks can be harder to deal with because in addition to that a sybil attacker can create multiple fake identities and it can even pretend that it forwards the message when in reality it is just sending it to itself.

Both attacks behave slightly different depending on the forwarding scheme (i.e. three-way-handshake or distributed forwarding) used by the underlying routing protocol. For the case of protocols such as IGF which uses a three-way-handshake, we describe below existing solutions provided by the SIGF protocol [19]. Moreover, we also explain our proposed solutions for protocols based on distributed forwarding such as BLR [5].

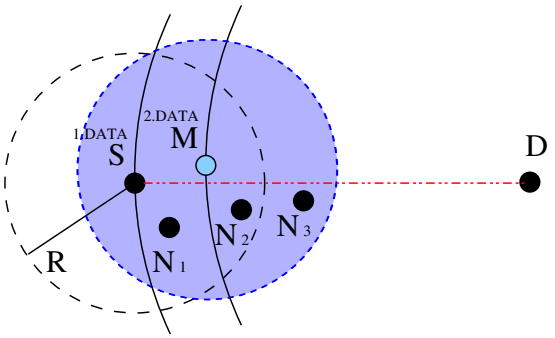
B. Sinkhole Attack in IGF and BLR

Here, we describe how the sinkhole attack affects both IGF and BLR according their forwarding schemes. Let's assume a current node located at position S and denoted as s that holds a data packet addressed to a destination d located at position D outside of its radio range (R). Let $N = \{n_1, n_2, \dots n_k\}$ be the set of neighbors of s, with each neighbor n_i being located at position N_i. To select its next hop s broadcasts a message indicating its position S. All neighbors located closer to d than s take part in the forwarding process. In unsecured environments, an attacker m located at position M inside the radio range R can pretend to be the best forwarding candidate in order to become the next hop.

Figure 1(a) shows the operation of a sinkhole attack in IGF forwarding. The current sender s broadcasts a short message (RTS) to ask for available neighbors. In these example n_1 and n_2. A sinkhole attacker m does not delay its response message (CTS) to pretend to be the one providing the most advance towards d. Thus, m cancels responses from n_1 and n_2 and s ends up sending the DATA message to m that drops it.



(a) Sinkhole attack in IGF



(b) Sinkhole attack in BLR

Fig. 1. In (a) a sender s uses the IGF protocol to forward a packet toward d in presence of a sinkhole attacker m. In (b) a sender s uses the BLR protocol to forward a packet toward d in presence of a sinkhole attacker m.

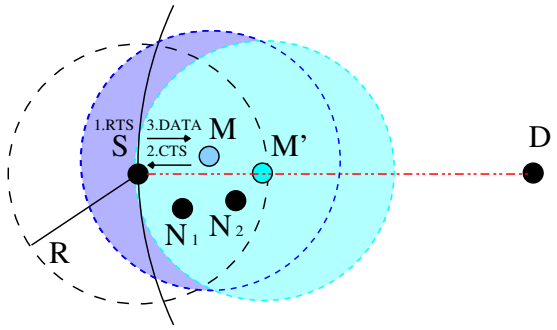
To avoid this sinkhole attack, SIGF proposes a contention window where s waits some time to receive more of one response (CTS). In addition, neighbors n_1 and n_2 do not cancel their responses even if some other neighbors answered first. Among all responses, s selects the neighbor n_2 whose position N_2 is the closest to d. SIGF also proposes a reputation mechanism to discard anomalous behavior as the one by the sinkhole attacker m that does not forward data packets.

Figure 1(b) shows the operation of a sinkhole attack in BLR forwarding. The current sender s broadcasts a unique DATA message including the packet and its position (S) to discover its neighbors (i.e. n_1 and n_2). Neighbors n_1 and n_2 compete in a distributed way delaying their forwarding of the data packet depending upon their progress towards d. A sinkhole attacker m can only cancel the forwarding of n_1 and n_2 by broadcasting the DATA message first. In this example, the forwarding performed by m cancels a neighbor n_2 located at position N_2 closer to d than M.

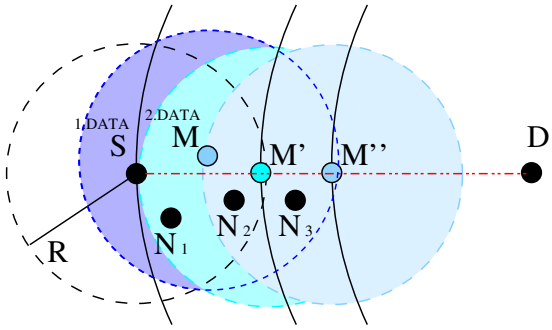
In this case, given that the node has to forward the DATA packet to act as relay, the attack is not very severe as the packet is not dropped. The only small issue is that it may require more hops as the position of M may not provide as many progress toward d as some of the neighbors (e.g. n_2) does.

C. Sybil Attack in IGF and BLR

Another interesting insider attack to consider is the sybil attack. In the sinkhole attack neighboring nodes can easily detect if the selected neighbor forwards the data packet or



(a) Sybil attack in IGF



(b) Sybil attack in BLR

Fig. 2. In (a) a sybil attacker m located at position M creates a false identity M' to become the next hop in the three-way handshake of s. In (b) a sybil attacker m located at position M creates a false identify M' to become the next hop in the distributed forwarding of s.

just drops it. However, a sybil attacker can create multiple identities to pretend that it forwards the data packet to a fictitious next hop, which is in fact itself, so that legitimate neighbors do not suspect from the attacker.

Figure 2(a) shows the operation of a sybil attack in IGF forwarding. The current sender s broadcasts a RTS message with its position S to discover its neighbors. A sybil attacker m receives the RTS message of s and creates a false identity for a node pretending to be located at position M', which is closer to d than the position of s. The attacker m chooses the false position M' as the closest position inside the radio range R of s to ensure that its response cancels that from all neighbors of s. Thus, m replies first with a CTS message including its false identity M'.

SIGF proposes a reputation scheme to control the behavior of nodes and detect sinkhole and sybil attacks. Nodes overhear the transmission of their neighbors and keep a reputation table in terms of forwarding success, location consistency, average delay, etc. So, a node penalizes a sinkhole attacker for not forwarding DATA messages. A node also penalizes a sybil attacker for changing its position in CTS messages. However, the sybil attacker can create multiple identities to fool the reputation scheme. Therefore, SIGF requires an additional cryptographic solution to verify the identities of nodes in the network.

Figure 2(b) shows the operation of a sybil attack in BLR forwarding. The current sender s broadcasts a DATA message including its position S to discover forwarding candidates. Neighbors n_1 and n_2 compete in a distributed way delaying their forwardings according to their progress towards d. A sybil attacker m creates a new identity pretending to be a node located at closest position M' toward d inside the radio range of s. Thus, m using its false identity broadcasts a DATA message to cancel the forwarding of n_1 and n_2. With this simple attack, there is not a big issue since n_3 receives the DATA message and continues the forwarding. However, the attack can be more elaborated by m creating an additional new identity with a false position M'' which is the closest inside its radio range R. Thus, after the forwarding with the identity located in M', the selected next hop is the other false identity M'', which now cancels not only n_1 and n_2 but also n_3.

To deal with this attack we present later on our solution which exploits the fact that even in this highly elaborated attack, n_1 detects an attack because it receives a DATA message from a position (M'') which is outside of its radio range.

IV. SBGR: Self-Protected Beaconless Routing

This section presents a self-protected beaconless geographic routing protocol that is able to deal with insider attacks in wireless sensor networks. SBGR is based on the Beacon-Less Routing Protocol (BLR [5]) proposed by Heissenbüttel et al. BLR provides an efficient distributed forwarding scheme that prevents almost all insider attacks, as discussed above. In the forwarding scheme employed by BLR the first forwarder cancels the possible forwardings of the rest of the neighbors. To guarantee that the forwarding is detected by all relay candidates, only nodes located in a particular area called Reuleaux-triangle are allowed to participate in the forwarding process. This area is defined so that in all possible positions inside the area all nodes can overhear each other. However, several studies [4] show that the distributed forwarding is prone to generating duplicate packets in realistic scenarios with transmission errors.

So, SBGR as an enhanced solution that includes two effective defenses against sinkhole and sybil attacks. It also incorporates a simple mechanism to avoid propagating duplicate packets in the case in which multiple neighbors forward the DATA packet.

Like in previous geographic routing protocols SBGR assumes that nodes are located in a known fixed-position. We also assume that the source of the packet uses some secure location service to determine the location of the destination [20] and that nodes check the integrity of the packets by overhearing during the distributed forwarding.

In the next subsections we illustrate the way in which our proposed protocol deals with sinkhole and sybil attacks as well as with duplicate messages.

A. Dealing with Sinkhole Attacks

Here, we describe a simple defense of SBGR against sinkhole attackers. The main idea is that neighbors must simply verify if they are located closer to the destination than the node that replied. In general, this would only happen for attackers which responded before their waiting time. That is, nodes only

cancel their waiting timers if they receive a response from a neighbor which is located closer to the destination than itself. For instance, in Fig. 1(b), the current sender s forwards a DATA message toward D. The Sinkhole attacker m broadcasts immediately to cancel all neighbors n_1 and n_2. In SBGR, n_2 realizes that its position N_2 is closer to the destination than the position of the attacker (M). Thus, n_2 ignores the broadcast of m and forwards the DATA message after its timer expires.

If the attacker reports a false position, we can deal with that as if it would have created another identity. So, we will explain that case in the remaining sections.

A side-effect of our solution to deal with sinkhole attackers is that it may generate duplicate packets. However, we can easily solve that problem without extra overhead. In particular, duplicates can be produced because some nodes located closer to the destination than the sinkhole attacker may forward the data packets while other neighbors providing more advance do the same because they didn't cancel their forwardings.

To solve this issue nodes store temporally the received packet along with the node that sent this message. For each duplicate received, a node checks if the current sender provides less advance than the stored sender. In this case, the node ignores the duplicate packet. Otherwise, the node resets its waiting timer and the message is saved with the current sender as the one providing the best advance. We also call that sender $BestRelay$.

The key aspect in this duplicate avoidance is that nodes in the next forwarding operations only consider the data packet from the $BestRelay$ at the previous forwarding operation. So, only a single relay is elected in the next round.

Figure 1(b) shows a common example of duplicate packets that appear in the presence of sinkhole attackers. A current sender s forwards a DATA message toward d. The Sinkhole attacker m broadcasts immediately the DATA message to cancel the forwarding from all legitimate neighbors n_1 and n_2. However, n_2 receives the broadcast of s and realizes that its position N_2 is closer to D than M. Thus, it does not cancel its transmission. In addition, the neighbor n_3 of the attacker m receives the broadcast from m and stores the message with BestRelay as M. It also sets its forwarding waiting timer according its position N_3. When the timer of n_2 expires it broadcasts the DATA message. In this case, n_3 receives a duplicate DATA message from n_2. Thus, n_3 realizes that its stored BestRelay M is further from D than the current sender N_2. So, n_3 resets its timer for the DATA message and updates its BestRelay as N_2. Thus is, all nodes would behave as if a single DATA message had been forwarded in the previous step (the one from n_2).

B. Dealing with Sybil Attacks

As we have explained before, sybil attacks are more difficult to deal with because nodes can create multiple identities pretending to be located at different positions from the real position of the attacker.

SBGR uses a constrained flooding of NOTIFY messages to make sure that DATA packets are forwarded towards the destination even in the presence of sybil attackers. The main idea is that neighbors which detect a sybil attacker (e.g. by suspecting of a false reported position after overhearing a message) start the dissemination of a NOTIFY message. The message is flooded within the coverage area of the potential attacker to make sure that legitimate nodes providing more progress than the false identity created by the attacker can receive the message and continue the routing task.

Fig 3 shows an example of the proposed solution that consist of 3 steps: detection, diffusion and recovery.

1) **Detection.** A current relay S sends a DATA message addressed to the destination D and a sybil attacker replies immediately pretending to be a node located at a false position M'. When a node such as X receives the DATA message (because the real position of the attacker is M) from a position M' which is outside its coverage area it suspects of a possible attack. Thus, X creates a NOTIFY message and starts the constrained flooding avoid the attack. The NOTIFY message includes the original DATA message and is augmented with the position of X. It also includes a new field called $ReliableRelay$ which is filled in with the $BestRelay$ associated to the DATA packet that initiated the detection. In our case, it is S which is the closest node to the destination (excluding the suspected attacker) from which X has received the DATA packet.
   To reduce the number of transmissions in the detection, only nodes that have already received the DATA message before are candidates to generate NOTIFY messages. Moreover, nodes use the same distributed forwarding mechanism used for data packet to forward NOTIFY messages. This means, that the first NOTIFY message which is sent cancels other NOTIFY messages from the remaining nodes that detected the issue. That is, the overall extra overhead of this proposed scheme is limited to a couple of messages.
2) **Diffusion.** To exit the sybil attacker's radio range, each node that receives the NOTIFY message and is closer to D than $ReliableRelay$ (e.g. Y), broadcasts the NOTIFY message. To reduce once more the overhead, only those nodes that received the DATA message and whose forwarding was canceled by the one from the attacker (M') are required to send the NOTIFY message.
3) **Recovery.** When the NOTIFY message reaches a node (e.g. W) that did not receive the DATA message included in the NOTIFY message, that means that W is outside the coverage area of the attacker and the DATA message can continue to be forwarded in the normal mode. So, such nodes extract the data message from the NOTIFY message and continue the forwarding. Again, to avoid a large number of similar data messages being routed, only those nodes which are closer to D than the position of $ReliableRelay$ in the NOTIFY message, extract and forward the DATA message.

The design of the constrained flooding considers the case in which a sybil attacker may use NOTIFY messages to reduce the performance of our proposal. First, the sybil attacker M can try to cancel the flooding of the NOTIFY message by

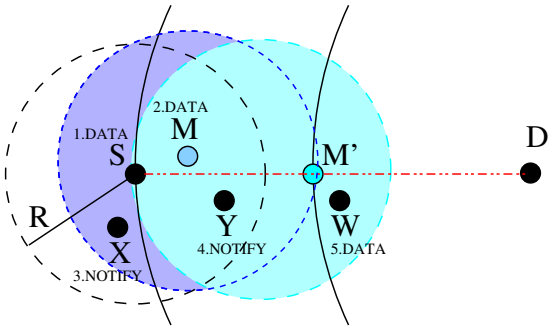


Fig. 3. SBGR using the Notify flooding to defend against Sybil attacks.

neighbors X and Y. So, M broadcasts immediately a NOTIFY message with a fake $ReliableRelay = M''$ whose position is closer to D than neighbors X and Y. To avoid the malicious cancellation, every node X that previously detected the sybil attack only cancels its transmission if it receives a NOTIFY message containing the same DATA and $ReliableRelay = S$. Then a node X broadcasts the NOTIFY message indicating a $ReliableRelay = S$ that guarantees the flooding for every neighbor Y in its forwarding area. Second, the sybil attacker M can try to disseminate duplicate NOTIFY messages to generate a broadcast storm in its coverage area. To avoid this unnecessary overhead, nodes only send a NOTIFY message per each DATA packet. Thus, nodes X and Y ignore duplicate NOTIFY messages transmitted from the sybil attacker M. To implement that in resource constrained sensor networks, nodes save only the identification tuple of each NOTIFY message transmitted consisting of the identifier and sequence of the source node that generates the data packet. Nodes store a temporal list of these tuples and when the list is full then it deletes the last recently used entry. So, nodes can discard the NOTIFY messages duplicated by a sybil attacker using few memory.

C. Algorithmic representation of SBGR Operation

SBGR provides a simple self-protected beaconless protocol being able to deal with insider attacks. SBGR is based on a reactive beaconless protocol (BLR) that avoids attacks compromising the routing information. The protocol uses two different forwarding schemes: distributed and flooding. The distributed forwarding only requires an unique DATA message per hop and avoids the interception of sinkhole attackers. The flooding forwarding uses a limited broadcast NOTIFY message to propagate the DATA messages beyond the area of influence of sybil attackers. Both forwarding schemes are shown in Algorithm IV.1 and Algorithm IV.2. These algorithms describe the operation of SBGR in four parts: the distributed forwarding of DATA messages, the detection of a false position, the flooding of a notify message and the recovery of a DATA message.

The distributed forwarding of the DATA message is illustrated in lines 1-9 of Algorithm IV.1. A node A receives a DATA message addressed towards D from node B. If A is closer to D than B and its saved $BestRelay$ is farther from D than B, A schedules its waiting timer based on its progress, saves the sender as $BestRelay$ and participates in the forwarding. If A does not receive any DATA message with a closer sender than the stored $BestRelay$, A broadcasts the DATA message when its waiting timer expires.

The detection of a false position is presented in lines 10-18 of Algorithm IV.1. If a node A receives a DATA message from B that is located outside of its radio range it creates a NOTIFY message where the field $ReliableRelay$ equals to its $BestRelay$ and sets a waiting time according to its distance to $ReliableRelay$. If A does not receive a NOTIFY message for the same data packet before its waiting timer expires it broadcasts the NOTIFY message to alert about the issue to neighboring nodes.

The flooding of a notify message is shown in lines 1-4 of Algorithm IV.2. When a node A receives a NOTIFY message referring to a saved DATA message for which its response was cancelled by another answer, and it is closer to D than the node in the field $ReliableRelay$, it rebroadcasts the NOTIFY

Algorithm IV.1 ProcessData(DATA, A, B, D): A receives a $DATA$ message addressed to D from B.

```
1:  if dist(A,B) <= R then
2:    if (A ∈ progressArea(B,D)) and (dist(B,D) < dist(bestRelay,D)) then
3:      bestRelay ← B
4:      t ← delayTimer(A,B,D)
5:      wait(t)
6:      if IsNotReceived(DATA) then
7:        broadcast(DATA)
8:      end if
9:    end if
10: else
11:   if (isSaved(DATA)) and (isNotSent(NOTIFY)) then
12:     t ← notifyTimer(A,bestRelay)
13:     wait(t)
14:     if isNotReceived(NOTIFY) or isNotSame(DATA,ReliableRelay) then
15:       broadcast(NOTIFY)
16:     end if
17:   end if
18: end if
```

Algorithm IV.2 ProcessNotify(NOTIFY, A, B, D, ReliableRelay): A receives $NOTIFY$ message with $ReliableRelay$ from B to D.

```
1: if isSaved(DATA) then
2:   if (dist(A,D) < dist(ReliableRelay,D)) and (isCancelledForwarding(DATA)) and (isNotSent(NOTIFY)) then
3:     broadcast(NOTIFY)
4:   else
5:     ProcessData(extract(NOTIFY),A,ReliableRelay,D)
6:   end if
7: end if
```

message. Note that this imposed condition limits the flooding to a very close area around the sender and the attacker.

Finally, the recovery of a DATA message from a NOTIFY message is shown in lines 5-7 of Algorithm IV.2. If a node A receives a NOTIFY message regarding a DATA message that the node does not store, this means that A is outside the radio range of the sybil attacker and can continue the distributed forwarding of the DATA message which is included in the NOTIFY message.

In conclusion, the simplicity of SBGR is based on the fact that nodes only require storing temporarily the messages received, without needing to keep neighborhood reputation, complex cryptographic material or location verifications. This makes the protocol to continue being as scalable as traditional geographic routing protocols, which is in fact the main salient feature of geographic routing.

V. Simulation Setup

This section compares the performance of Self-Protected Beaconless Geographic Routing (SBGR) and SIGF, which is the best performing solution in the literature. Our evaluation shows the performance of both protocols in the presence of sinkhole and sybil attacks. For comparison, we use the version of SIGF that has local history and reputation without cryptographic mechanisms. The configuration of SIGF is the same used by its authors. That is, 60^o forwarding areas, fixed collection window equals 3 messages, include destination is active. Next hop selection is done by reputation, and limited to high reputation neighbors with the following parameters $\alpha = 5/8, \beta = 1/8, \gamma = 1/8, \zeta = 1/8, R_{threshold} = 0.45$. The reader can refer to [19] for details.

For SBGR and SIGF we use $MaxDelayTime = 300ms$ and the maximum number of DATA retransmissions to protect against weak radio links is set to 5.

We simulate sinkhole and sybil attackers that behave exactly as in the models we have described in our previous analysis. That is, in SIGF and SBGR sinkhole attackers reply immediately without delay. In each forwarding, a sybil attacker creates a new identity with the closest position inside the radio range of the current relay and replies immediately.

The simulation scenario is a 2000x2000m^2 area with an increasing number of attackers (15 to 40) which are randomly added to the simulation. The analysis focuses on the effects of attacks. Thus, nodes are evenly distributed in the area to ensure that only greedy forwarding of packets (i.e. no need of perimeter routing to avoid void areas) is enough to deliver the packets to destinations. The area is divided into telleselated-hexagons where nodes are located randomly until reaching a mean density of 20 neighbors/node. For each scenario, we simulate 100 random sources sending a 110 byte packet to a destination located at the middle of the network. As network simulator we use TOSSIM [21] which considers collisions and uses a realistic MAC layer. In addition, we include a Packet Reception Ratio (PRR) model derived from previous studies [22]. The results are the average of 50 simulation runs in order to achieve a sufficiently small 95% confidence interval.

A. Performance metrics

We considered the following metrics during the evaluation of performance of the algorithms:

- Packet Delivery Ratio. It shows the percentage of packets that reach the destination node. This metric determines the robustness of the protocols against attackers.
- Number of Packets per Hop. It measures the average number of packets transmitted by a relay and its neighbors to forward the data message to the next relay.
- Tx Packets per Delivery. It estimates the average number of packets used in the routing process from a source until reaching the destination. This determines the efficiency of each protocol.
- Number of Hops. It indicates the average length of the route from every source to the destiantion.
- Time per Hop. It measures the time needed for the relay and neighbors to forward the packet to the next relay.

B. Effect of the number of sinkhole attackers

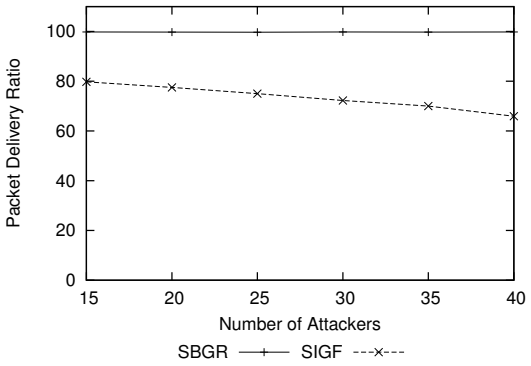
These results measure the performance of both protocols in networks with transmissions errors and a mean number of 20 neighbors per node. We also increase the number of Sinkhole attackers. Fig. 4(a) shows the packet delivery ratio (PDR). SBGR clearly outperforms SIGF regardless of the number of attackers. In particular SBGR shows that it is very effective at dealing with sinkhole attackers, making the PDR reach a 100%. SIGF with reputation needs several forwardings to detect a malicious node dropping the packets. At increasing number of attackers, SIGF lowers its PDR because in each next hop selection the probability of selecting a Sinkhole attacker increases.

Fig. 4(b) shows the number of transmissions per hop for each of the message types. SBGR also has a lower number of transmissions per hop (i.e. overhead) than SIGF. While the distributed distributed forwarding of SBGR only requires one transmission per hop, the three-way handshake used by SIGF requires at least 4 transmissions: RTS, CTS, DATA and ACK. In addition, to to avoid the selection of the first sinkhole response, SIGF uses a collection window requiring receiving at least 2 additional responses per hop.

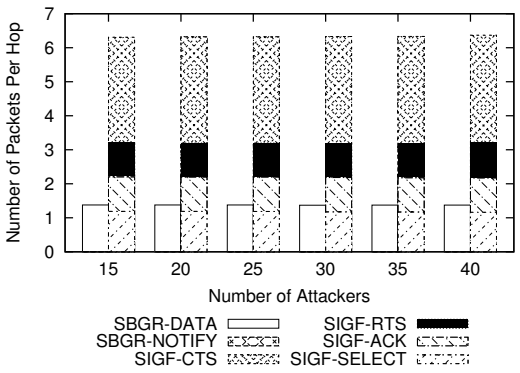
To analyze the efficiency of both protocols Fig. 4(c) shows the total number of transmissions per destination successfully reached. Again, SBGR needs a lower total number of transmissions than SIGF in all the simulated scenarios. The reason is that in SBGR sinkhole attackers forward the DATA message immediately to try to cancel forwardings from neighbors and generate duplicate packets. However, SBGR has an efficient performance because nodes use their stored $BestRelay$ to avoid propagating duplicate packets. As the number of attackers increases SIGF increases the number of transmissions per destination reached. The reason is that the number of failed deliveries increases, making the packet forwardings of undelivered messages useless.

C. Effect of the number of sybil attackers

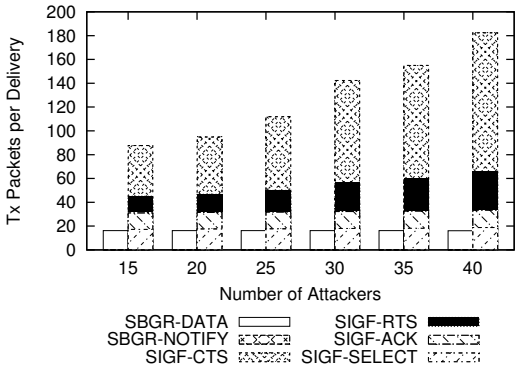
In this case, the difference in performance is even bigger because as our results show, SIGF is not able to deal with sybil



(a) Delivery Rate

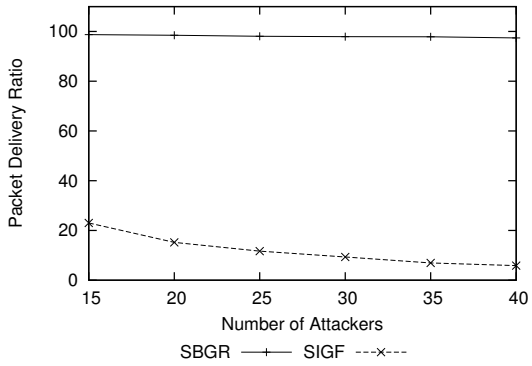


(b) Packets per hop

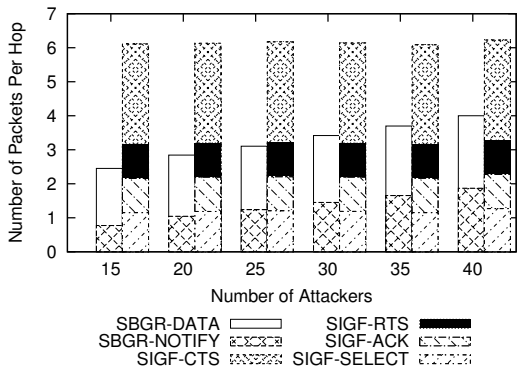


(c) Tx Packets per Delivery

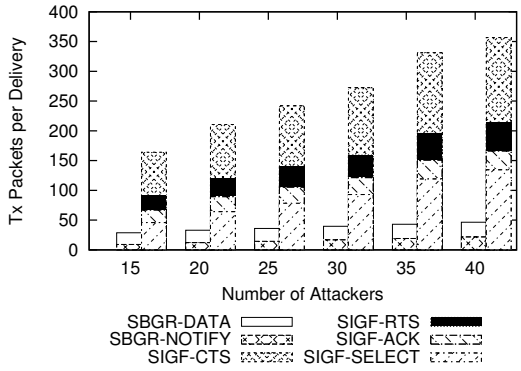
Fig. 4. Statistics with 20 neighbors at increasing the number of Sinkhole attackers.



(a) Delivery Rate



(b) Packets per hop



(c) Tx Packets per Delivery

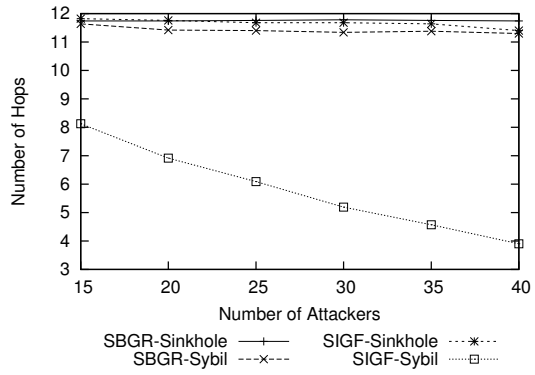
Fig. 5. Statistics with 20 neighbors at increasing the number of Sybil attackers.

attacks. Reputation schemes are not able to avoid attacks from nodes with multiple identities.

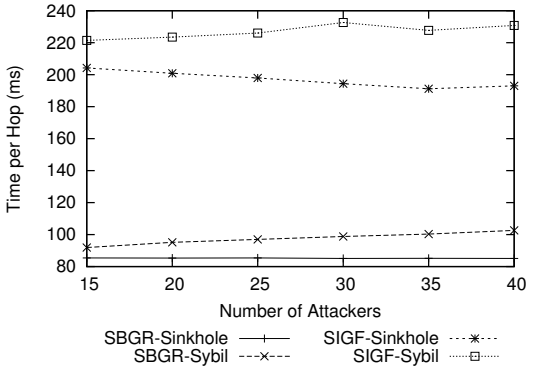
Fig. 5(a) shows that SBGR clearly outperforms SIGF in terms of the packet delivery ratio.

As we mentioned, the problem of SIGF is due to the fact that reputation schemes are ineffective to fight sybil attackers that intercept and drop all packets in their radio range. The reason is that sybil attackers use different false identities in each forwarding with the closest position from the current sender to the destination. Thus, the reputation scheme is not able to find enough evidence about the wrong performance of a particular node. In SIGF, the packet is only delivered if no Sybil attacker is in the path toward the destination. Therefore, at increasing the number of attackers, the probability of reaching the destination is dramatically reduced. SBGR keeps nearly a 100% delivery ratio demonstrating that the proposed solution is quite effective.

To measure the overhead required by SBGR to achieve such a high packet deliver ratio, Fig. 5(b) compares the number of transmissions per hop. We can see that as expected SBGR increases moderately the number of transmissions as the number of attackers increases. This is because of the flooding of NOTIFY messages. In any case, this flooding is limited inside the radio range of sybil attackers. So, in all cases, the number of packets per hop in our simulations never goes beyond 4, which is still below the number of messages



(a) Number of hops



(b) Hop-to-Hop Time

Fig. 6. Statistics with 20 neighbors at increasing the number of attackers: Sinkhole and Sybil

required by SIGF.

To show the effectiveness of the protocol Fig. 5(c) shows the average number of transmissions per successful delivery to the destination. Even though SBGR has a much higher delivery ratio than SIGF, SBGR requires a lower number of transmissions than SIGF. The results show the good balance achieved by SBGR with a perfect delivery ratio with only a moderate overhead of control messages.

D. Effects of attackers in overall delay and hop count

In this section, we show the performance of both protocols in terms of the hop-by-hop forwarding time and the average number of hops to reach the destination.

Fig. 6(b) shows the time per hop required by both protocols. SBGR requires a lower time than SIGF. The reason is that SBGR uses a distributed forwarding based on neighbors competing to transmit first. SIGF delays the forwarding by needing several responses to select explicitly the next hop. When considering different attacks, we can see that in general sybil attacks make the protocol take more time per hop. In the case of SBGR this is due to the fact that nodes detecting the attacker send out NOTIFY messages and that processing requires some time until the message bypasses the attacker. But even in that case SBGR still requires less time per hop than SIGF.

Fig. 6(a) shows the mean number of hops in successful deliveries. SBGR and SIGF use the same number of hops because they use the same selection function based on the proximity toward the destination. The only notable difference is the case of sybil attackers in which SIGF has a much lower number of hops towards the destination. However, it is not due to a good performance, but to the fact that SIGF only delivers the message to the destination when no sybil attacker is present, and that only tends to happen when sources and destinations are very close.

VI. Conclusions and Future Work

We present a Self-Protected Beaconless Geographic Routing (SBGR) to deal with insider attacks in WSNs. SBGR provides an efficient protocol to ensure the delivery of packets to the destinations in the presence of insider attackers and transmission errors.

SBGR includes two simple mechanisms to protect data delivery against sinkhole and sybil attackers. In the distributed forwarding, nodes avoid sinkhole attackers by not cancelling their forwarding of DATA messages if they provide more advance than the sinkhole attacker. The constrained flooding of NOTIFY messages is used to defend against sybil attackers that create false identities with closer position to the destination and to pretend that messages were in fact forwarded. In this case, nodes detect the false positions and propagate a NOTIFY message in the radio range of the sybil attacker in order to reach new nodes which are beyond the radio range of the sybil attacker. In SBGR, nodes only require storing temporarily the state of recently received messages.

The results of our simulations show that SIGF is ineffective to protect against sinkhole and sybil attacks. SIGF needs a learning time to detect the malicious behavior in the reputation scheme. Moreover, SIGF is not able to detect sybil attackers that create new identities in each forwarding.

Unlike SIGF, SBGR is able to obtain almost 100% delivery ratio even in networks with an important number of sinkhole and sybil attackers. In addition, SBGR has a lower overhead in terms of required number of transmissions than SIGF. The results show that SBGR provides an efficient and reliable communication solution for wireless sensor applications deployed in insecure environments.

VII. Acknowledgments

This work has been partially supported by the MOTEGRID project (PII1C09-0101-9476).

References

[1] H. Oliveira, E. Nakamura, and A. Loureiro. Directed position estimation: A recursive localization approach for wireless sensor networks. In *In Proceedings of the 14th IEEE International Conference on Computer Communications and Networks*, San Diego, USA, 2005.

[2] A. Rao, S. Ratnasamy, C. Papadimitriou, S. Shenker, and I. Stoica. Geographic routing without location information. In *MobiCom '03: Proceedings of the 9th annual international conference on Mobile computing and networking*, pages 96–108, New York, NY, USA, 2003. ACM.

[3] Brian Blum, Tian He, Sang Son, and Jack Stankovic. IGF: A state-free robust communication protocol for wireless sensor networks. Technical report, Department of Computer Science, University of Virginia, USA, 2003.

[4] J. Sanchez, P. Ruiz, and R. Marin-Perez. Beacon-less geographic routing made practical: challenges, design guidelines, and protocols. *Communications Magazine, IEEE*, 47(8):85–91, 2009.

[5] Marc Heissenbüttel and Torsten Braun. A novel position-based and beacon-less routing algorithm for mobile ad-hoc networks. In *In Proceedings of the 3rd IEEE Workshop on Applications and Services in Wireless Networks, (ASWN' 03)*, pages 197–210, Bern, Switzerland, July 2003.

[6] M. Zorzi and R. R. Rao. Geographic random forwarding (geraf) for ad hoc and sensor networks: Energy and latency performance. *IEEE Transactions on Mobile Computing*, 2(4):349–365, 2003.

[7] Paolo Casari, Michele Nati, Chiara Petrioli, and Michele Zorzi. Efficient non-planar routing around dead ends in sparse topologies using random forwarding. In *ICC'07*, pages 3122–3129, 2007.

[8] Stefano Basagni, Michele Nati, Chiara Petrioli, and Roberto Petroccia. Rome: Routing over mobile elements in wsns. In *GLOBECOM*, pages 1–7, 2009.

[9] Chris Karlof and David Wagner. Secure routing in wireless sensor networks: Attacks and countermeasures. *Elsevier's AdHoc Networks Journal, Special Issue on Sensor Network Applications and Protocols*, 1(2–3):293–315, September 2003.

[10] Alessandro Mei and Julinda Stefa. Routing in outer space: fair traffic load in multi-hop wireless networks. In *Proceedings of the 9th ACM international symposium on Mobile ad hoc networking and computing*, MobiHoc '08, pages 23–32, New York, NY, USA, 2008. ACM.

[11] Loukas Lazos and Radha Poovendran. Serloc: secure range-independent localization for wireless sensor networks. In *WiSe '04: Proceedings of the 3rd ACM workshop on Wireless security*, pages 21–30, New York, NY, USA, 2004. ACM.

[12] E. Shi and A. Perrig. Designing secure sensor networks. *Wireless Communications, IEEE*, 11(6):38–43, 2004.

[13] Adrian Perrig, Robert Szewczyk, J. D. Tygar, Victor Wen, and David E. Culler. Spins: security protocols for sensor networks. *Wirel. Netw.*, 8(5):521–534, 2002.

[14] Chris Karlof, Naveen Sastry, and David Wagner. Tinysec: a link layer security architecture for wireless sensor networks. In *SenSys '04: Proceedings of the 2nd international conference on Embedded networked sensor systems*, pages 162–175, New York, NY, USA, 2004. ACM.

[15] Naveen Sastry, Umesh Shankar, and David Wagner. Secure verification of location claims. In *WiSe '03: Proceedings of the 2nd ACM workshop on Wireless security*, pages 1–10, New York, NY, USA, 2003. ACM.

[16] Srdjan Capkun and Jean pierre Hubaux. Secure positioning of wireless devices with application to sensor networks. In *In Proceedings of InfoCom*, 2005.

[17] Zang Li, Wade Trappe, Yanyong Zhang, and Badri Nath. Robust statistical methods for securing wireless localization in sensor networks. In *IPSN '05: Proceedings of the 4th international symposium on Information processing in sensor networks*, page 12, Piscataway, NJ, USA, 2005. IEEE Press.

[18] A. Boukerche and Xu Li. Atrm: An agent-based trust and reputation management scheme for wireless sensor networks. In *In Proceedings of IEEE Global Telecommunications Conference*, pages 1857–1861, 2005.

[19] Anthony D. Wood, Lei Fang, John A. Stankovic, and Tian He. Sigf: a family of configurable, secure routing protocols for wireless sensor networks. In *SASN '06: Proceedings of the fourth ACM workshop on Security of ad hoc and sensor networks*, pages 35–48, New York, NY, USA, 2006. ACM.

[20] Joo-Han Song, Vincent W.S. Wong, and Victor C.M. Leung. A framework of secure location service for position-based ad hoc routing. In *PE-WASUN '04: Proceedings of the 1st ACM international workshop on Performance evaluation of wireless ad hoc, sensor, and ubiquitous networks*, pages 99–106, New York, NY, USA, 2004. ACM.

[21] Philip Levis, Nelson Lee, Matt Welsh, and David Culler. TOSSIM: Accurate and Scalable Simulation of Entire TinyOS Applications. *Proceedings of the First ACM Conference on Embedded Networked Sensor Systems, (SenSys 2003)*, November 2003.

[22] Juan A. Sanchez, Rafel Marin-Perez, and Pedro M. Ruiz. BOSS: Beacon-less On Demand Strategy for Geographic Routing in Wireless Sensor Networks. In *Proc. of the 4th IEEE International Conference on Mobile Ad-hoc and Sensor Systems (MASS '07)*, pages 1–10, October 2007.