Layout: T1 Standard SC | Book ID: 218207_1_En | Book ISBN: 978-1-4471-2154-1
Chapter No.: 19 | Date: 11-8-2011 | Page: 1/7

A Distributed Scheme to Detect Wormhole Attacks in Mobile Wireless Sensor Networks

Oya Simsek and Albert Levi

Abstract Due to mostly being unattended, sensor nodes become open to physical attacks such as wormhole attack, which is our focus in this paper. Various solutions are proposed for wormhole attacks in sensor networks, but only a few of them take mobility of sensor nodes into account. We propose a distributed wormhole detection scheme for mobile wireless sensor networks in which mobility of sensor nodes is utilized to estimate two network features (i.e. network node density, standard deviation in network node density) through using neighboring information in a local manner. Wormhole attack is detected via observing anomalies in the neighbor nodes' behaviors based on the estimated network features and the neighboring information. We analyze the performance of proposed scheme via simulations. The results show that our scheme achieves a detection rate up to 100% with very small false positive rate (at most 1.5%) if the system parameters are chosen accordingly. Moreover, our solution requires neither additional hardware nor tight clock synchronization which are both costly for sensor networks.

Keywords Mobile wireless sensor networks · Security · Wormhole attacks

This work was supported by the Scientific and Technological Research Council of Turkey (TUBITAK) under grant 110E180.

O. Simsek (✉) · A. Levi
Sabanci University, Orhanli, Tuzla, 34956 Istanbul, Turkey
e-mail: oyasimsek@su.sabanciuniv.edu

A. Levi
e-mail: levi@sabanciuniv.edu

E. Gelenbe et al. (eds.), *Computer and Information Sciences II*,
DOI: 10.1007/978-1-4471-2155-8_19, © Springer-Verlag London Limited 2011

Layout: T1 Standard SC | Book ID: 218207_1_En | Book ISBN: 978-1-4471-2154-1
Chapter No.: 19 | Date: 11-8-2011 | Page: 2/7

1 Introduction

As a result of significant advances in hardware manufacturing and wireless communication technology along with efficient software algorithms, wireless sensor networks [1] emerged as a promising network infrastructure for various applications. Due to being mostly unattended and the open nature of wireless communication channels, sensor nodes become open to physical attacks which may lead to various attacks including wormhole attack. In wormhole attack, an attacker tunnels messages received in one part of the network over a wormhole link and replays them in a different part of the network. This low-latency tunnel attracts network traffic on the wormhole link which can empower the attacker to perform traffic analysis, denial of service attacks; collect data to compromise cryptographic material; or just selectively drop data packets through controlling these routes using the wormhole link. Moreover, an attacker can perform this attack without compromising any legitimate nodes, or knowing any cryptographic materials since the attacker neither creates new packets nor alters existing packets.

There are several approaches for wormhole detection in wireless sensor networks which mostly focus on static networks. These solutions are mainly based on detecting the maximum distance any message can travel, or the maximum time of travel of any message [2], discovering one-hop neighbors in a secure way [3], or monitoring the data traffic of neighbor nodes [4]. Also, most of these approaches require additional hardware (e.g. directional antennas in [5], GPS in [2], a specialized hardware for one-bit challenge request-response [3] protocol), special trusted nodes such as guards in [6], highly accurate time or location measurements [3], or tight clock synchronization [2], which seems infeasible for large scale wireless sensor networks because of its resource limitations and economic costs. In this paper, we propose a distributed wormhole detection scheme for mobile wireless sensor networks. Our scheme aims to utilize the mobility feature of the sensor nodes to examine the environment and network properties, and derive new features which help understanding the network better.

2 Proposed Scheme

Our scheme includes two main phases: (1) stabilization, and (2) detection phases. Stabilization phase is for sensor nodes to collect information from the network through using neighboring information to estimate the node density of the network locally, d_i^r, for node i at rth round, and to compute the standard deviation of the change in the estimated node density, σ_i^r. This phase runs once right after the uniform random deployment of the sensor nodes. In detection phase, based on the pre-computed statistical values, the detection mechanism is activated to check for anomalies in the network, and detected nodes are revoked from the network. Without a wormhole attack being performed, the difference between the number of

Layout: T1 Standard SC | Book ID: 218207_1_En | Book ISBN: 978-1-4471-2154-1
Chapter No.: 19 | Date: 11-8-2011 | Page: 3/7

neighbors of a node and its estimated network density does not exceed the standard deviation of its network density. However, under wormhole attack, this difference can be higher due to fake neighboring connections, especially when a node is close to the wormhole ends.

2.1 Network Assumptions and Threat Model

The network is composed of mobile nodes having same communication range as well as same physical properties. The sensor nodes are deployed randomly using uniform distribution in the sensing area. None of the nodes know their location information. Nodes can obtain the neighbor count information of their neighbors as well as their own neighboring information. Secure neighbor discovery is out of the scope of the paper. There are proposed solutions for neighbor discovery, [7, 8], addressing node mobility as well as energy efficiency in the literature. Necessary link level security requirements (i.e. confidentiality, authentication, and integrity) are assumed to be fulfilled by the lower layers. It is sufficient for an attacker to capture two legitimate nodes and create a low-latency tunnel between them. We assume that the wormhole link is bidirectional. In other words, both ends of wormhole link overhear the packets; tunnel these packets to other node via this low-latency tunnel so that the receiving node can replay these packets at that end of the wormhole. The attacker may drop the packets selectively in a random way. However, by doing so, the wormhole link becomes less attractive and this is not a desired situation for the attacker. Thus, we assume that the attacker does not drop any packets.

2.2 Details of the Proposed Scheme

Stabilization Phase. Stabilization phase starts right after the uniform random deployment of N sensor nodes, and runs S rounds. In a round, each node discovers their neighbors securely, broadcasts its neighbor count, and locally computes statistical features of the network (i.e. d_i^r and σ_i^r) after receiving all neighbor counts of its neighbors.

Share Neighboring Information. When a node learns its neighbors, it broadcasts an information packet including its own identity, i, and the number of its neighbors, Ψ_i. This information is critical while estimating the network features.

Calculate and Update Statistical Metrics. After all nodes share the number of their neighbors, each node i has the following information: its own neighbors, N_i, the number of its own neighbor number, Ψ_i, and neighbor count information of its neighbors, $\Psi_j, \forall j \in N_i$. Then, node i computes the network density, d_i^r, and standard deviation in d_i^r, σ_i^r, in a local way using equations (initial conditions are $d_i^0 = 0$ and $\sigma_i^0 = 0$):

Layout: T1 Standard SC | Book ID: 218207_1_En | Book ISBN: 978-1-4471-2154-1
Chapter No.: 19 | Date: 11-8-2011 | Page: 4/7

$$d_i^r = \frac{\Psi_i + \sum_{j \in N_i} \Psi_j}{\Psi_i + 1} \times (1 - \alpha) + d_i^{r-1} \times \alpha \quad (1)$$

$$\sigma_i^r = \sqrt{\frac{1}{\Psi_i + 1} \times \left[\left(\sum_{j \in N_i} \left(\left(\Psi_j - d_i^{r-1} \right)^2 \right) \right) + \left(\Psi_i - d_i^{r-1} \right)^2 \right] \times (1 - \alpha) + \alpha_i^{r-1} \times \alpha} \quad (2)$$

We use exponential averaging, which we are inspired by its usage in TCP round trip time estimation, to give more importance to the latest data retrieved from neighbors without losing the previous calculated values. α and $(1 - \alpha)$ are the weights which are used to estimate standard deviation and local network density of a node. At each round, each node estimates a candidate density value which is calculated by averaging the neighbor counts received from neighbors along with its own neighbor count (Eq. 1). After that, the node updates its density via using the exponential average of the previous value and the new estimated value. The procedure is same for the calculation of standard deviation in the node density (Eq. 2).

Detection Phase. In detection phase, pre-computed network features along with round threshold, T_{round}, (i.e. the maximum number of rounds in which a node a needs to witness an anomaly about a node b to keep node b in its local suspected nodes list), alarm threshold, T_{alarm}, (i.e. the minimum number of alarm to broadcast a node as globally *suspected*), and revocation threshold, T_{revoc}, (i.e. the number of nodes required to revoke a node), are used to detect the anomaly created by the wormhole link. A round in detection phase is composed of neighbor discovery, sharing the number of neighbors, testing detection criteria along with broadcasting specific messages when necessary, and finally revocation of detected nodes.

Check for Suspicious Nodes based on Statistical Metrics. After obtaining the neighborhood information, each node i has locally-estimated network density, d_i^s, and locally-estimated standard deviation in d_i^s, σ_i^s, and the neighboring information $\Psi_j, \forall j \in N_i$. To detect an anomaly, node i first checks whether the number of its own neighbors exceeds d_i^s more than σ_i^s. If the difference exceeds σ_i^s, it accuses its neighbors and adds them to its list which is for tracking locally suspicious nodes. Otherwise, node i checks its neighbors one by one with the same method to detect a suspicious behavior and updates its list accordingly. If the alarm counter for a locally suspected node j exceeds T_{alarm}, then node i broadcasts a message deeming j is a globally *suspected* node. If any node in the list of locally suspected nodes does not show an anomaly during T_{round}, then node i deletes that node from its list. When a node i receives an alarm saying node j is a potential malicious node, it runs the following check: If j is already in its globally suspected nodes list, it updates the alarm counter of j; otherwise, it adds j to the list. To revoke node j, the number of nodes deeming node j as suspected must exceed T_{revoc} which is basically a preset percentage of the total number of nodes in the network.

Layout: T1 Standard SC | Book ID: 218207_1_En | Book ISBN: 978-1-4471-2154-1
Chapter No.: 19 | Date: 11-8-2011 | Page: 5/7

Revoke Detected Node. A globally *suspected* node can be revoked from network through node self-destruction mechanisms proposed in [9] and [10]. When a node i receives a message saying node j is a malicious node, it sends a message to the base station for revocation of j and updates its list which is for keeping track of revoked nodes accordingly.

3 Performance Evaluation

We analyzed the performance of our scheme via simulations, and present our results in a comparative way. We analyzed the effects of the change in the system parameters on the detection rate under the simulation setup defined below. Due to limitation of space, only a small subset of the simulation results is included in the paper.

The results presented in the graphs are average of 20 simulations. $N = 200$ nodes are distributed over a field of $A = 100$ m $\times$ 100 m. We use random movement model in which each node chooses a random direction; and moves towards it with a uniformly distributed random speed in the range of (5, 15 m/s). Nodes have a communication range of 15 m. We simulated various values of T_{alarm} and T_{revoc}. The results show that the more optimal and stable value for α is 0.5. Therefore, we choose α as 0.5 in our simulations. We assume that 5% of all nodes are static all the time. Also, we assume that wormhole attack is not performed during stabilization phase. Stabilization phase runs once and lasts $S = 1{,}000$ rounds. Detection phase runs during the lifetime of a sensor node due to the possibility of wormhole attack being performed at any time. However, we limit this value to 2,000 rounds in our simulations.

Detection and false positive rates are our main metrics while evaluating the success of the simulations. Detection rate is the ratio of the number of simulation runs where the wormhole is detected successfully, $D\#$, over total number of simulation runs, $S\#$, which is computed as $D\#/S\#$. False positive rate per simulation run is computed as the ratio of falsely detected nodes, $F\#$, over total node number, N. False positive rate is the average of this ratio of all simulation runs, hence, it is computed as $\frac{\sum_1^{S\#}\left(\frac{F\#}{N}\right)}{S\#}$.

If T_{alarm} increases, node i needs to witness more suspicious behavior of node j to broadcast it as globally *suspected*, and detection probability of wormhole decreases considering the mobility of the nodes. Since nodes are mobile, they may not be under the effect of wormhole for such long time to exceed that high T_{alarm} value for a suspected node. Hence, there may not be enough nodes to broadcast that suspected node as globally *suspected*. The number of revoked nodes decreases, thus, detection and false positive rate decreases. Similarly, T_{revoc} is inversely proportional to the number of revoked nodes since high T_{revoc} means more nodes are required to agree on revoking a node. The simulation results which are presented in Figs. 1 and 2 verify those observations. Increasing T_{alarm} or T_{revoc}

Layout: T1 Standard SC | Book ID: 218207_1_En | Book ISBN: 978-1-4471-2154-1
Chapter No.: 19 | Date: 11-8-2011 | Page: 6/7

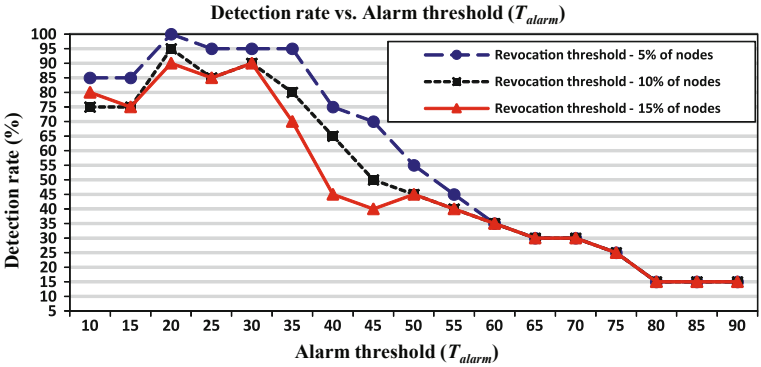

Fig. 1 Detection rate versus Alarm threshold (T_{alarm}) for $T_{\text{revoc}} = 10$, $T_{\text{revoc}} = 20$, and $T_{\text{revoc}} = 30$; $T_{\text{round}} = 20$; wormhole ends are chosen randomly

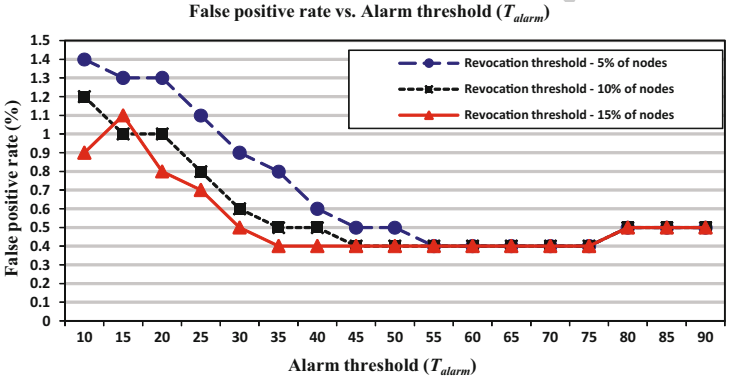

Fig. 2 False positive rate versus Alarm threshold (T_{alarm}) for $T_{\text{revoc}} = 10$, $T_{\text{revoc}} = 20$, and $T_{\text{revoc}} = 30$; $T_{\text{round}} = 20$; wormhole ends are chosen randomly

decreases the detection and false positive rates, but they do not change much after a high enough T_{alarm} value.

4 Conclusions

In this paper, we propose a distributed wormhole detection scheme for mobile wireless sensor networks which utilizes mobility of sensor nodes to detect wormhole attack to estimate new features in a local way which helps understanding the network better. Wormhole attack is detected via observing anomalies in the neighbor nodes' behaviors based on these estimated network features and

Layout: T1 Standard SC | Book ID: 218207_1_En | Book ISBN: 978-1-4471-2154-1
Chapter No.: 19 | Date: 11-8-2011 | Page: 7/7

the neighboring information. We analyzed the performance of proposed scheme via simulations using different system parameters. The results show that our scheme achieves a detection rate up to 100% with very small false positive rate (at most 1.5%) if the system parameters are chosen accordingly. Moreover, our solution requires neither additional hardware nor tight clock synchronization which are both costly for sensor networks.

References

1. Akyildiz, I.F., Su, W., Sankarasubramaniam, Y., Cayirci, E.: Wireless sensor networks: a survey. Comput. Netw. **38**(4), 393–422 (2002)
2. Hu, Y.C., Perrig, A., Johnson, D.B.: Packet leashes: a defense against wormhole attacks in wireless ad hoc networks. IEEE INFOCOM **3**, 1976–1986 (2003)
3. Capkun, S., Buttyan, L., Hubaux, J.: SECTOR: secure tracking of node encounters in multi-hop wireless networks. SASN, pp. 21–32 (2003)
4. Khalil, I., Bagchi, S., Shroff, N.B.: LITEWORP: a lightweight countermeasure for the wormhole attack in multihop wireless networks. DSN, pp. 612–621 (2005)
5. Hu, L., Evans, D.: Using directional antennas to prevent wormhole attacks. NDSS, pp. 22–32 (2004)
6. Lazos, L., Poovendran, R., Meadows, C., Syverson, P., Chang, L.W.: SeRLoc: secure range-independent localization for wireless sensor networks. Wise, pp. 21–30 (2005)
7. Kohvakka, M., Suhonen, J., Kuorilehto, M., Kaseva, V., Hannikainen, M., Hamalainen, T.D.: Energy-efficient neighbor discovery protocol for mobile wireless sensor networks. Ad hoc Netw. **7**(1), 24–41 (2009)
8. Bagchi, S., Hariharan, S., Shroff, N.: Secure neighbor discovery in wireless sensor networks. ECE Technical Reports. Paper 360 (2007)
9. Curiac, D.-I., Plastoi, M., Banias, O., Volosencu, C., Tudoroiu, R., Doboli, A.: Combined malicious node discovery and self-destruction technique for wireless sensor networks. SENSORCOMM, pp. 436–441 (2009)
10. Plastoi, M., Curiac, D.-I.: Energy-driven methodology for node self-destruction in wireless sensor networks. SACI, pp. 319–322 (2009)