VOL. 10, NO. 9, MAY 2015 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

PROTECTING SOURCE LOCATION PRIVACY AGAINST WORMHOLE ATTACK USING DAWN IN WIRELESS SENSOR NETWORKS

S. R. Naresh, S. V. Gayathri Soumiya and A.V. Ramprasad
Department of ECE, KLN College of Engineering, Madurai, India
E-Mail: nareshsr@yahoo.com

ABSTRACT

As sensor-driven applications become progressively more integrated into our lives; issues linked to sensor privacy will become increasingly important. In wireless sensor networks, adversaries can make use of the traffic information for locating the monitored objects. Network coding has been shown to be an efficient approach to improve the wireless system performance. In a wormhole attack, the attacker can forward each packet using wormhole links and without modifies the packet transmission by routing it to an unauthorized remote node and pose a severe threat to many functions in the network, such as routing and localization. We developed a wormhole attack and are prevented by DAWN (Distributed detection Algorithm against Wormhole attack in wireless Network coding systems) algorithm using hash operation in cryptosystems. Simulation and methodical results reveal that our scheme acquires low energy consumption and less false positive rate than hotspot attack.

Keywords: DAWN, cryptosystems, hotspot attack, wormhole attack, wireless sensor networks.

1. INTRODUCTION

A wireless sensor network (WSN) of spatially distributed autonomous sensors which is used to monitor physical or ecological conditions, such as sound, temperature, pressure, etc. and to cooperatively pass their data through the network . The more modern networks are bi-directional, the more control of sensor activity is possible. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrialized process monitoring and control, machine health monitoring, and etc. WSN consists of hundred/thousand wireless nodes distributed with geographical area, as all wireless nodes collect information and supply it towards the central node for further processing . Here, the distributed nodes sense the activity/current status of its region and supply to the next upper node which collects different information from different nodes. The final information is supplied to the central node to remove the redundant information and further processing. Wireless Sensor Networks are networks made up of tiny embedded devices. Each device is capable of sensing, processing and communicating. Wireless Sensor Networks are frequently ad hoc, meaning that nodes can be added at any time and configure themselves to be part of the existing network. Any node can act as a relay to pass messages in the network. This works sound for applications that add new sensors to replace those that have used up their battery life, or need to add more nodes for better coverage.

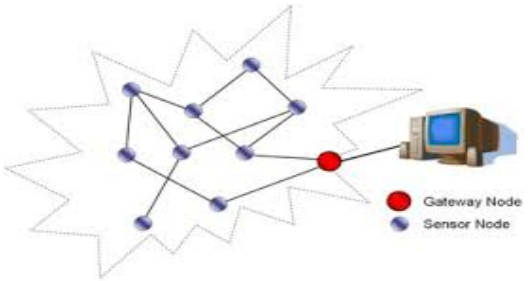

Figure-1. Wireless sensor network model.

The source location privacy-preserving schemes can be classified into global-adversary-based and routing-based schemes. The global-adversary-based schemes assume that the adversary can monitor every radio transmission in every communication link in the network. To preserve source node's location privacy, each node has to send packets from time to time. If a node does not have sensed data at one time slot, it sends dummy packet, so that the adversary cannot know whether the packet is for a real event or dummy data. However, the assumption that the adversary can monitor the transmissions of the entire network is not realistic, especially when the WSN is deployed in a large area. Moreover, if the adversary has a global view to the network traffic, he can locate pandas without making use of the network transmissions. Transmitting dummy packets periodically consumes a significant amount of energy and bandwidth, and decreases packet delivery ratio due to increasing packet collision, which makes these schemes impractical for WSNs with limited-energy nodes.

Generally sensor networks are deployed to monitor the endangered animals in a forest. An event is triggered whenever an animal is patterned in the monitored area. The seeker tries to collect this information and may capture the animal in danger of extinction. The above scenario depicts the weakness of WSNs is more

because of its open wireless medium to transmit the information from source to destination.

In the efforts to advance the system performance of wireless networks, network coding has been shown effectively and it constitutes a different approach compared to traditional networks, where intermediate nodes store and forward packets as similar to the original. In contrast, in wireless network coding system, the forwarders are permitted to apply encoding schemes on packets what they receive, and thus they transmit new packets. The idea of mixing packets on each node takes good advantages of the opportunity diversity and broadcast nature of wireless communications, and significantly enhances system performance.

. The wormhole attack is one of these attacks. Ina wormhole attack, the attacker can forward each packet using wormhole links and without modifies the packet transmission by routing it to an unauthorized remote node. Hence, receiving the rebroadcast packets by the attackers, some nodes will have the illusion that they are close to the attacker. With the ability of changing network topologies and bypassing packets for further manipulation, wormhole attackers pose a severe threat to many functions in the network, such as routing and localization. To investigate wormhole attacks in wireless network coding systems, we focus on their impact and countermeasures in a class of popular network coding system, in order to utilize best resources, before data transmissions, routing decisions are made based on local link conditions by some test transmissions.

The rest of this paper is organized as follows. We review the related works in Section II. The network and wormhole attack models are discussed in Section III. Section IV will describe our wormhole attack detection algorithm- DAWN. In Section V, we will show the effectiveness and robustness of our solutions. Our experiments and the related study are also discussed. In Section VI, we will conclude this paper.

2. RELATED WORKS

Recently, location privacy in wireless and wired networks has gained much attention. Different schemes have been developed to protect users' privacy in location tracking systems which determine the user's positions for location-based services. Location privacy in these schemes is content oriented, where location information is unruffled and protected as the user's private data.

Routing-based schemes preserve source nodes' location privacy by sending packets through different routes to make back tracing the movement of the packets from the Sink to the source nodes infeasible. In [3] and [4], a random-walk-based privacy-preserving scheme, called Phantom, is proposed. Each packet takes a random walk to a random location before it is sent to the Sink. However, the scheme fails if the adversary's overhearing range is more than thesensornodes' transmission range. Moreover, it is very likely that routes will loop around the source node and branch to random location that is not far from the node. To resolve this problem, the source node can attach the direction of the random walk to the packet header, and each node in the random-walk route forwards the packet to a random neighbor in the same direction. However, once a packet is captured in the random-walk route, the adversary can know the direction information to the source node, which lessens the difficulty of tracing the packets back to the source.

Global-adversary-based schemes [5], [6] assume that adversaries can monitor the traffic of the entire network. Each node has to periodically send packets, and send dummy packets if it does not have sensed data so that it is infeasible for the adversaries to differentiate between the real and dummy packets. However, if the nodes increase the time interval of packet transmission to lessen the energy cost of the dummy packets, the packet delivery delay rises. This is attributed to the fact that if an event is sensed between two time slots, the node should wait the first time slot to transmit the event. To alleviate the tradeoff between the overhead of dummy packets and packet delivery delay, Shao *et al.* [7] propose a statistically strong source privacy-preserving scheme. The nodes send the real packets as soon as possible with keeping them statistically indistinguishable from the dummy packets.

Network coding has been shown to be an effective approach to increase the wireless system performance. However, security issues impede its wide deployment in practice. Moreover the well-studied pollution attacks; there is one more severe threat that is wormhole attacks, which weakens the performance gain of network coding. Since the underlying features of network coding systems are distinctly different from traditional wireless networks, the influence of wormhole attacks and countermeasures are generally unknown. In this paper, we quantify wormholes' distressing harmful impact on network coding system performance through experiments. We rigorously prove that DAWN guarantees a good lower bound of successful detection rate. We perform study on the resistance of DAWN against collusion attacks. We discover that the robustness depends on the node density in the network, and prove a necessary condition to attain collusion-resistance. DAWN doesn't rely on any position information, global synchronization assumptions or extraordinary hardware/middleware. It is only based on the confined information that can be obtained from ordinary network coding protocols, and thus the transparency of our algorithms is bearable.

3. NETWORK AND ADVERSARY MODELS

3.1 Network model

As illustrated in Figure-2, the considered WSN consists of the Sink and a large number of homogeneous panda-detection sensor nodes which are randomly deployed in an area of interest. The Sink and the sensor nodes are stationary. The sensor nodes are resource-constrained devices with low battery power and computation capacity, but equipped with sensing, data processing, and communicating apparatus. The sensor nodes are interconnected through wireless links to perform

distributed data collection. The Sink has sufficient computation and storage capabilities to perform two basic functions: 1) broadcasting beacon packets to bootstrap our scheme; and 2) collecting the data sensed by sensor nodes. Pandas have embedded radiofrequency (RF) tags [8], and when a sensor node senses a panda, the node is called a source node and generates and sends event packets to the Sink. Each sensor node has transmission radius of rS meters and the communication in the network is bidirectional, i.e., any two nodes within the wireless transmission range can communicate with each other. Multihop communication is employed if the distance between a sensor node and the Sink is more than rS, where some sensor nodes (called relaying nodes) act as routers to relay the source node's packets. The Sink is the sole destination for all the event packets.

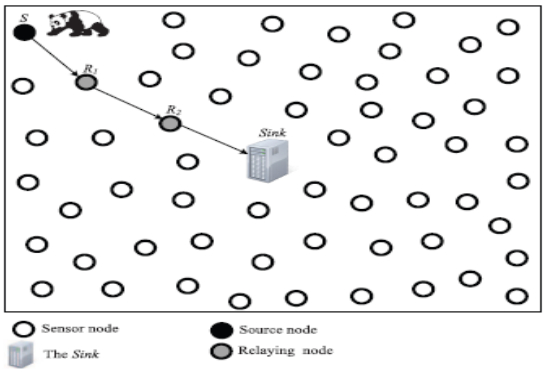

Figure-2. The architecture of the considered WSN.

3.2 Wormhole attack model

In wormhole attacks, the attackers between distant locations transmit packets using an out-of-band tunnel. The transmission tunnel is called a wormhole link. The packet loss rate on the wormhole link is negligible. When the wormhole attack initiate, the attackers can detain data packets on either side, forward them through the wormhole link and rebroadcast them on the other node.

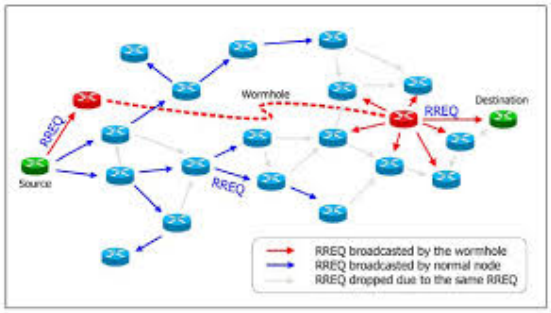

Figure-3. Wormhole attack model.

4. THE DISTRIBUTED DETECTION ALGORITHM

In this section, we consider a practical scenario where centralized authority cannot be found. We propose DAWN, a distributed algorithm to detect wormhole attacks in wireless network coding systems. We will perform rigorous study on the detection rate of our algorithm and its resistance against collusions.

4.1 Algorithm design

The basic idea of DAWN is based on the result that any two nodes in the neighborhood, the one with lower ETX are supposed to receive novel packets prior to the other one with high probabilities. In other words, innovative packets are transmitted from low ETX nodes to high ETX nodes with high probabilities. In order to examine the innovative packets transmission direction, nodes will work collaboratively. In particular, DAWN has two phases on each node:

1) *Report* packets direction observation results to its neighbors and

2) *Detect* whether any attackers exist.

Algorithm: The distributed detection algorithm for wormholes in wireless network coding systems (dawn) on node U

Input: R: the set of reports recognized in the last batch; N (u): the set of u's neighbors; sj: the local observation result of each neighbor
j ∈ N (u); δ: the threshold.
Output: Detected wormhole attacker in N (u), if any.

1: **for** Each report r(i; j; k) ∈ R **do**
2: **if** ETX(j) − ETX(i) ≤δ OR i =∈ N(j) **then**
3: Discard this report;
4: **else**
5: **if** j ∈ N(u) **then**
6: sj ← sj + 1;
7: end if
8: **if** k < 2 **then**
9: Forward this report r(i; j; k + 1);
10: **end if**
11: **end if**
12: **end for**
13: **for** each v ∈ N(u) **do**
14: Let C(v)={i |i ∈ N(v) s.t. ETX(v) − ETX(i) > δ}
15: **if** sv ≥ ⌈(|C(v)|+1)/2⌉ **then**
16: Mark v as a detected wormhole attacker, and block any traffic from or to node v in future batches.
17: **end if**
18: **end for**

A. Report phase

For each node, it will suspect that one neighbor is an attacker if it receives novel packets from the neighbor but the ETX of this neighbor is much higher than that of itself (i.e., the distance between the ETXs is greater than the threshold δ). It sends its judgment as a report to its neighbors. A node is called a judge node of a neighbor if the distance between their ETXs is greater than the threshold. Each report r is a tuple as Equation (1).

R = (time, A suspect, A self, K pub, S novel, sig) (1)

Here, time is when the reporting node discover the asymmetrical transmission. A suspect is the address of the suspected node, which sends out a novel packet and owns a higher ETX than the recipient's. A self is the address of the reporting local node. Since any node can alter the report when forwarding it, we need to apply cryptographic techniques to protect the uprightness of the reports. We use digital signatures of the reports to defend against malicious modification, and abstract of the novel packet for administrative verification. Thus, we introduce symmetric cryptographic scheme into our system to make it more robust against attacks. In Equation 1 K pub is the public key of the reporting node. S novel is the set of the signatures of the received novel packets. Sig is the signature of the report. The signatures are produced as Equation (2).

Sig = Encrypt (K sec, (Hash (P)) (2)

Here K sec is the secret key of the reporting node. P is the novel packet that was received from the target.

B. Detect phase

For each node in the Detect phase, it receives reports from the judge nodes of any potential attackers. It first examine whether a report is from a valid judge node. If so, it will forward the report unless it has previously been forwarded twice. Three-hops of the reports make sure that more reachable neighbors of the potential attacker will hear this report. The detection algorithm on each node gathers and calculates the number of its judge nodes who launch report about the reported potential attacker in the current batch. If the number of judge nodes composes the majority, the node will make the decision that the attacker is involved in a wormhole attack and obstruct it from future communications.

5. SIMULATION

To evaluate the efficiency and effectiveness of DAWN, we have developed an ns2 simulator for network coding systems by creating network of around 100 nodes and implemented our algorithms in the simulator.

The simulation results given demonstrate that the false positive probability decreases and the detection probability increases when the monitoring device's overhearing radius increases. This is because the adversary can monitor more nodes and collect more accurate traffic information. This is also true when the number of monitoring devices increases.

In our scheme, the powerful adversary who has a large number of monitoring devices with large overhearing radius will not locate hotspots. The few times the adversary could locate the hotspot were random. As we have discussed earlier, using cryptosystems is necessary to prevent packet correlation and using fake packets can boost source nodes' location privacy preservation. To lessen the energy cost, our scheme uses energy efficient cryptosystems, together with hash function and symmetric key cryptography, and avoids the widely energy consuming asymmetric-key cryptography. We can see that the hashing algorithm in cryptosystems consume low energy Since the Sink has more computational and energy capabilities than the sensor nodes, the nodes in the route between a fake source node and the Sink encrypt the packets but the Sink removes the encryption layers instead of using encryption and decryption operations at each node. The overhead can be further lessened by encrypting the packets at some nodes instead of all the nodes in the route. Pseudonyms do not require large storage space or computational power in our scheme, because they can be computed by the efficient hashing operations. Finally, we compared the energy, false positive ratio and detection ratio between wormhole attack and hotspot attack.

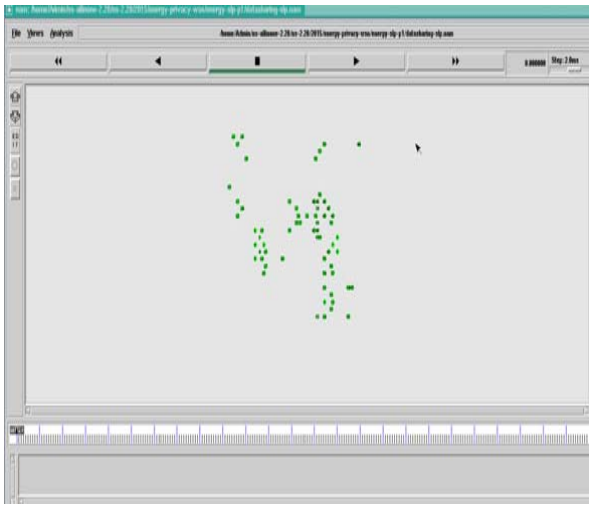

Figure-4. Initialization of node creation.

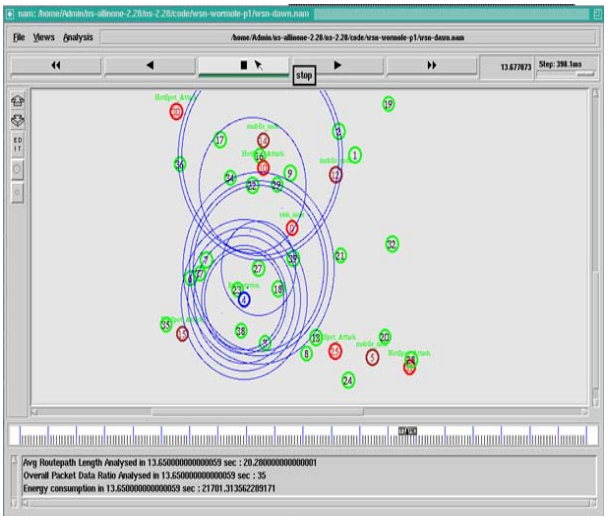

Figure-5. Prevention of wormhole attack.

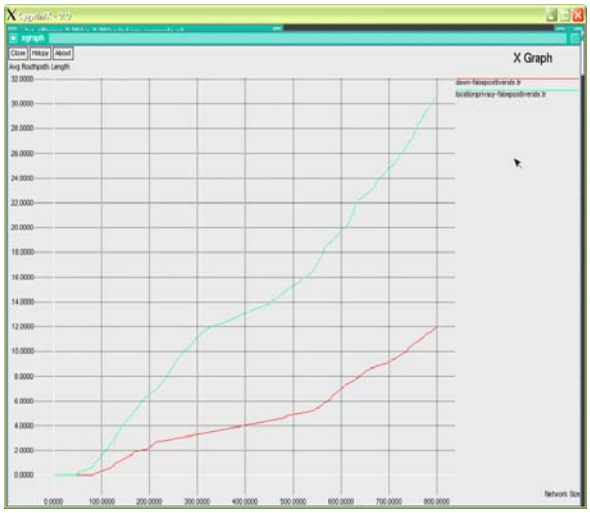

Figure-6. Comparison of false positive ratio between location privacy and DAWN.

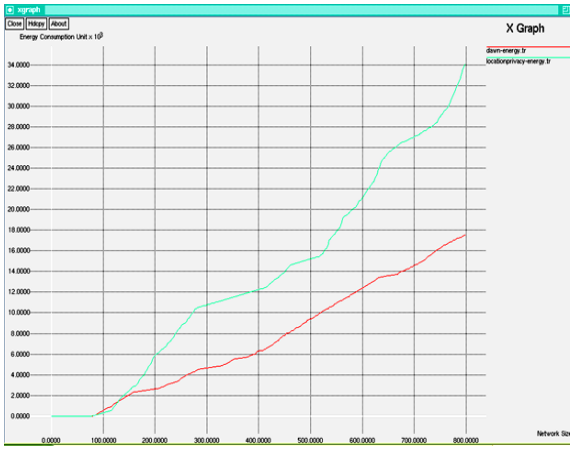

Figure-7. Comparison of energy between location privacy and DAWN.

Figure-8. Comparison of detection ratio between location privacy and DAWN.

6. CONCLUSIONS

We have introduced a novel attack to locate source nodes in WSNs, called wormhole attack, which uses a realistic adversary model. For the distributed wireless network, we proposes DAWN, Distributed detection Algorithm against Wormhole in wireless Network coding systems, by exploring the alteration of the flow directions of the innovative packets caused by wormholes. We have shown that even if the adversary does not have a global view to the network traffic, we can locate hotspots using few monitoring devices and simple traffic study techniques. Our simulation and analytical results have demonstrated that the wormhole attack has energy utilized as well as false positive rate is lower than hotspot attack. Moreover, our scheme can provide a strong protection against wormhole attack using hash algorithm in cryptosystems with efficient usage of energy. In future, this work can be extended for other attacks also and additionally we can add sink location privacy too.

REFERENCES

[1] Shiyu Ji, Tingting Chen and Sheng Zhong. 2014. "Wormhole Attack Detection Algorithms In Wireless Network Coding Systems", IEEE Infocom 2014 - IEEE Conference on Computer Communications, May.

[2] Mahmoud M.E.A. Mahmoud and Shen(Sherman) Shen. 2012."A Cloud-Based Scheme For Protecting Source- Location Privacy Against Hotspot-Locating", IEEE Transactions On Parallel And Distributed Systems, Vol. 23, No. 10, October.

[3] M. Shao, Y. Yang, S. Zhu and G. Cao. 2008. "Towards Statistically Strong Source Anonymity for Sensor Networks," Proc. IEEE Infocom '08, pp. 51-59, April.

[4] Y. Yang, M. Shao, S. Zhu, B. Urgaonkar and G. Cao. 2008. "Towards Event Source Unobservability With Minimum Network Traffic In Sensor Networks," Proc. First Acm Conf. Wireless Network Security (Wisec '08), pp. 77-88, April.

[5] S. R. D. R. Maheshwari, J. Gao. 2007. "Detecting Wormhole Attacks In Wireless Networks Using Connectivity Information," in IEEE Infocomm.

[6] B. Hoh and M. Gruteser. 2005. "Protecting Location Privacy through Path Confusion," Proc. First Int'l Conf. Security And Privacy For Emerging Areas N Comm. Networks (securecomm '05), pp. 194-205, September.

[7] P. Kamat, Y. Zhang, W. Trappe and C. Ozturk. 2005. "Enhancing Source Location Privacy In Sensor Network Routing," Proc. IEEE Int'l Conf. Distributed Computing Systems (Icdcs '05), Pp. 599-608, June.

[8] C. Ozturk, Y. Zhang and W. Trappe. 2004. "Source-Location Privacy in Energy Constrained Sensor Network Routing," Proc. Second Acm Workshop Security of Ad Hoc and Sensor Networks (Sasn '04), pp. 88-93.

[9] S. Tilak, N. Abu-Ghazaleh and W. Heinzelman. 2002. "A Taxonomy of Wireless Micro-Sensor Network Models," Acm Sigmobile Mobile Computing And Comm. Rev., Vol. 6, No. 2, pp. 28-36, April.