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

www.arpnjournals.com

# AMPUTATING WORMHOLE ATTACK IN WIRELESS SENSOR NETWORK USING SWARM INTELLIGENCE

Thanga Mariappan L.[1] and Ruba Soundar K.[2]
[1]Information Technology, Sree Sowdambika College of Engineering, Aruppukottai, India
[2]Department of Computer Science and Engineering, P.S.R Engineering College, Sivakasi, India
E-Mail: thangamariappanme@gmail.com

**ABSTRACT**

In wireless sensor networks (WSNs), due to the restricted resources of the nodes, are highly vulnerable to attacks at all network layers; however, the so-called "wormhole attack" is particularly challenging because it resists self-protective measures exclusively based on cryptographic protocols, this attack that not only diminishes the network capacity but also affects the reliability of information being transmitted. No emphasis was made towards the preventing the wormhole attack. In this paper a swarm-based framework that uses the security agents and security officer nodes. Preserving the legitimate packets coming from reserved route only, thereby discarding the contaminated packets has been proposed from another network.

**Keywords:** wormhole attack, cryptographic protocols, security agents, security officer node, swarm-based network.

## 1. INTRODUCTION

A typical wireless sensor network is expected to give a certain data that the user is actively enquiring about after some amount of time. Many attack schemes tend to stop the proper performance of sensor networks to delay or even prevent the delivery of data requested by user. Despite the fact that the term attack usually refers to an adversary's attempt to disrupt, undermine, or destroy a network, a Wormhole attack refers to any event that diminishes or eliminates a network's ability to perform its expected function. Such a technique may be helpful in specific applications such as utilizing the best of these attacks to find the weak tips of presented protocols at different layers.

These attacks consequently would expose weaknesses that lead to effective countermeasures. Understanding these vulnerabilities can develop techniques for identifying attacks that attempt to take advantage of them and implement mechanisms to mitigate these attacks. In other more serious applications, there are situations where network blocking is necessary to protect public safety.

Consider a large-scale wireless sensor network in which a massive number of wireless sensor nodes are randomly distributed in the target area. Directed Diffusion is the underlying protocol. The network consists of a large number of sensor nodes such as MICA2 sensors. Every sensor node has limited capabilities in terms of computation, storage, and wireless communication. The sensor nodes operate on non-renewable batteries; once a node exhausts its battery it is considered to be dead. We assume that the sensors are physically insecure, since the physical access to the motes is probabilistically possible in hostile environments. The user interacts with the network through a data collection unit, called a sink. A sink or base station could be any arbitrary sensor node that can inject quires (interests) to propagate along the network. The queries may be optimized or otherwise processed at the place of injection and then they are disseminated in the sensor network using multi-hop communication according to some query processing mechanism. Sensor nodes whose sensing results match the query disseminate data reports back to the sink over potentially multi-hop wireless links. Wormhole attack that tunnel information from one to another network, that is it get the data from one network replicate it into another network through tunnel that particular network may confused due to this action. At that time hacker may easily enter and do misuse inside the network. Among the variety of threats and risks that wireless LANs are facing, wormhole attack occurs more common and serious ones. When a wormhole attack occurs, an attacker forces base station to confuse and terminate its connection to nodes of the particular network by first compromising the AP`s MAC address. Current techniques by detecting wormhole attack using swarm intelligences are mainly based on spoof able and predicable parameters such as sequence numbers, which can be guessed by the attackers. To enhance the reliability of intrusion detection systems swarm based networks are used, Swarm intelligence is a collective behavior of self-organized systems, natural or artificial. The proposed idea is based on finding wormhole attack by means of Swarm Intelligence.

## 2. RELATED WORKS

Wormhole attack prevention using clustering and digital signatures in reactive routing of open medium, absence of infrastructure, dynamic network topology, cooperative algorithms, lack of centralized monitoring and resource constraints, ad hoc networks are vulnerable to many kinds of attacks, among which wormhole attack is chosen as the topic of discussion. A novel technique based on clustering and digital signatures for prevention against wormhole attacks without use of special hardware, time synchronization or dependency on time or hop difference between colluding nodes to identify attacked routes. Statistical wormhole detection for mobile sensor networks attack is one of the most challenging yet detrimental security issues in mobile wireless sensor networks (MWSNs). However, as most of the existing

countermeasures are designed mainly for fixed WSNs using hardware devices or information of entire WSNs (topology or statistical), they cannot be effectively used in MWSNs. As SWAN utilizes the localized statistical neighborhood information collected by mobile nodes, it apprehends wormholes not only without requiring any special hardware device but also without causing significant communication and coordination overhead. Two-Level Secure Re-routing (TSR) in Mobile Ad Hoc Networks static infrastructure, open nature and node mobility causes several issues in Mobile Ad Hoc Network (MANET), such as energy utilization, node authentication and secure routing. In this paper we propose a new scheme, Two-level Secure Re-routing (TSR), an attack resilient architecture for Mobile Ad hoc networks. It is significantly different from existing solutions, as it does not focus on any specific attack, but instead, taking a general approach it achieves resilience against a wide range of routing disruption DoS attacks. TSR is a double-layer scheme that detects attacks at the transport layer but responds to them at the network layer. The potential applications and pervasive nature of mobile ad-hoc networks (MANETs) has made them an attractive target for attackers. The wireless medium of communication coupled with constrained resources enable attacks which can be executed by a weak adversary. A wormhole is one such attack which poses considerable threat, particularly to routing protocols.

## 3. METHODOLOGY

### 3.1. Characterize the nodes

First describe the model to characterize a Wormhole attack in the wireless network.

To characterize the attacks, consider two nodes involved in a transmission. We use the commonly used statistical model from ITU (International Tele-communication Unit) recommendations. The ratio of the received and transmitted powers, $P_r$ and $P_u$ respectively, in dBm is given by

$$L=\frac{Pr}{Pu}(dBm) = K+ \gamma \log_{10} d+\varphi_{dBm}+ \phi_{dBm} \quad (1)$$

Where $\gamma \log 10$ d models the path loss as a function of the distance d between the transmitter and receiver. Also, $\gamma$ is the path loss exponent and K is a unit less constant. The attenuation from shadowing, φdBm, is normally distributed with zero mean and variance $\sigma^2_{\varphi}$. The values of the parameters γ, K and $\sigma^2_{\varphi}$ depend on the propagation environment. φdBm represents the variation caused by small scale fading and can be modeled as a Raleigh (for non line-of-sight (non-LOS) channels) or Rican (for LOS channels) distribution with appropriate parameters which depend on the propagation environment. Next we develop a mathematical model for wormhole attack using swarm intelligences events. For ease of analysis, continuous time signal models are used. Although our final detection algorithms are implemented using discrete signal models, discretization has no effect on the optimality of the detector. We assume that both the user and attacker can be mobile or static.

For infrastructure networks, we denote the distance between the user and the AP by $d_0(t)$ and the distance between the attacker and the AP by $d_1(t)$. $d_0$ and $d_1$ are continuous functions of time t. Unless the movement patterns of the attacker and the user are symmetrically exact, $d_1(t) \neq d_0(t)$. Suppose a wormhole attack using swarm intelligences occurs at time $t_0$.

Let

$$d_1(t_0)=d_0(t_0)+\Delta d=d_0(t_0)\left(1+\frac{\Delta d}{d0(t0)}\right) \quad (2)$$

We assume that the user and attacker are in environments with propagation parameters [Ki,γ i, φi, øi] where i=0 for the user and i=1 for the attacker. The monitored signal strength x(t) is given by

$$x(t) = N(t) + f(t) = N(t) + \Delta m \cdot u(t - t0) \quad (3)$$

where f(t) represents the signal and N(t) is the noise u(t) is the unit step located at unknown time instance $t_0$. The jump amplitude of f(t) at $t_0$ is $\Delta m=K_1-K_0+\gamma_1 \log_{10} d_1(t_0)-\gamma_0 \log_{10} d_0(t_0)$ and

$$N(t)=\begin{cases} N_1(t), & t<t_0; \\ N_2(t), & t\geq t_0; \end{cases}$$

Where

$$N_1(t) =K_0+\gamma_0 \log_{10} d_0(t)+\varphi_0+ \phi_0 \quad (4)$$

$$N_2(t)=K_0+\gamma_0 \log_{10} d_0(t_0)+\gamma_1 \log_{10}\frac{d1(t)}{d1(t0)} + \varphi 1 + \phi 1 \quad (5)$$

By this method we can easily come to know that our network has been attacked by the attackers or not. To develop detection mechanism in wireless sensor networks by correlating the signals transmitted to the Access Points. If our network is affected, we can prevent the attack by the following Methodology

### 3.2. Coordinated filters design

While transmitting signal from node to Access Point it may contains some fading effects of the wireless network. Note that small scale fading causes variations in the received signal strength within the order of one wavelength and is therefore a high frequency component. Shadow fading causes variations in the order of tens of wavelengths. Path loss is caused by spatial movements in the order of hundreds of wavelengths and corresponds to the low frequency component. This motivates us to divide the whole frequency domain of N (t) into three frequency subsets as

$W=w1 \cup w2 \cup w3,$

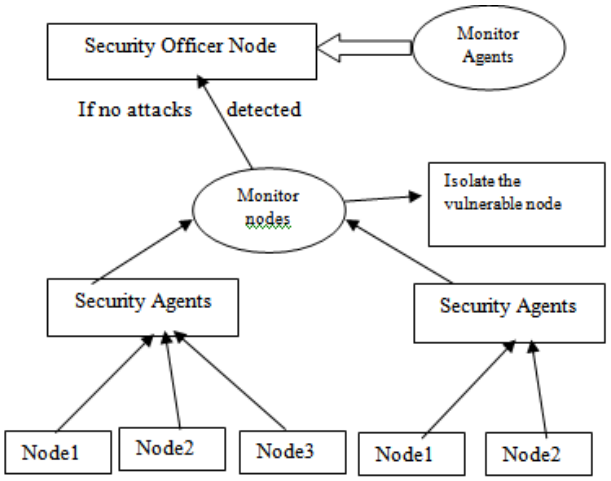
where w1,w2 and w3 are the frequency ranges of small scale fading component N1(t), shadow fading component N2(t) and path loss component N3(t), respectively.
Since

N(t) = N1(t) + N2(t) + N3(t)
N1(t),N2(t),N3(t) are mutually independent,
$S_N(w) = S_N1(w) + S_N2(w) + S_N3(w)$.

This Signal to noise ration can be diminished because every network may contain some noise, so limited variations will be accepted. The matched filter is used for the detection of vulnerable nodes Not only with the frequency of signal strength we used some QoS parameters such as throughput, packet ratio will be trained to the security agents.

### 3.3. Swarm scrutinization

Here with some security related mechanisms will be used, the swarm agents such as decentralized agents will be trained with the quality of parameters these agents will act as access points, and it monitors the nodes present in the wireless sensor network. These parameters are maintained only with the Agents.




If no attacks detected Security Agents will change the QoS parameters randomly and it should be informed to the legitimate nodes through key exchange algorithm such as Elgamal cryptosystem. One more centralized node Security officer node is used here to monitor the security Agents. There may be a chance of compromising the security agents. So securing the network again one more security officer node is used to monitor the security agents.

### 3.4. Bayesian hypothesis test

Our detection problem in wavelet domain can be summarized as follows. Let the observed wavelet detail coefficient y transformed from x(t) at time $k = t_0 2^j$ and scale j(≥ 1) have the form y = s+n, where $s = \Delta m 2^{j/2} |I_\psi(0)|$ and $n \sim \eta(0,\sum)$,with$\sum = C2(j)2j$ . The noise n has a Gaussian distribution because it has approximately constant power lever $C_2(j)2^j$. Our aim is to detect the signal s from Gaussian noise n.
The hypotheses to be tested are:

- $H_0$[null] : $Y \sim \eta_0(0, \sum)$
- $H_1$[alternative] : $Y \sim \eta_1(s, \sum)$

We assume that there exists a priori probability associated with the hypothesis: P(H0) = π and P(H1) = 1 - π. For simplicity, we assume that $c_{ij}$ , the cost incurred by choosing hypothesis $H_i$ when hypothesis $H_j$ is true, has uniform cost. The likelihood ratio test between $H_0$ and $H_1$ is $L(y) = \frac{p1(y)}{p0(y)}$. Thus the corresponding Bayesian decision rule can be proved to have a form as follows,

$$\delta_B(y) = \begin{cases} 1, \text{if } y \geq \frac{s}{2} \\ 0, \text{if } y < \frac{s}{2} \end{cases}$$

Given a signal strength trace x[n] = [x1, xM], our algorithm is described by the following steps:
**1) step-1:** Use DWT to obtain the detail coefficients d(j, k)at observation scale j = 5.
**2) step-2:** Compare d(j, k) with threshold $Thr_j = \frac{s}{2}$
**3) step-3:** Generate alarm if d(j, k) > Thrj for some k.

The scale j = 5 is proved to achieve the highest detection rate in our testing scenarios. The threshold
$Thr_j = \frac{s}{2} = \min\{\Delta m\} 2^{j/2-1} |I(0)|$ for scale j
where |I (0)| = 0.5.

The value of min Δm is obtained empirically for each environment and is given in Section V. The detector performance varies with the observation scale. Given a certain value of Δm, the highest detection rate is achieved at the optimal scale. Our model does not consider the impact of interference from other users on the received signal strength. This is because in the presence of interference, the AP will not be able to successfully receive the packet. Thus it will not associate the packet with any user and the corresponding signal strength measurement will not be used by the detection algorithm. If the interference is so small that the packet is correctly received, the magnitude of the interference is expected to be small enough to be neglected (for example, the IEEE802.11b standards require an SNR of 10dB for successful reception at 11Mbps).

**Table-1.** Upper bound on the false alarm rate.

| observation scale j | 4 | 5 | 6 | 7 |
|---|---|---|---|---|
| false alarm rate | 0.0137 | 0.0274 | 0.1065 | 0.2054 |

### 3.5. Prevention by path selection algorithm

The vulnerable nodes can be easily detected by the previous methodologies after finding the wormhole attack we should block the tunnel through which the attack carried, for that we have to use path selection algorithm for that particular hacker node.

1. At time instant k, a bandwidth request r arrives between nodes I and j.
2. Run the available bandwidth estimation algorithm links with no bandwidth estimation available.
3. Compute the best path using the shortest widest path algorithm with weights as calculated in step 2.
4. Obtain the available bandwidth A on the bottleneck link of the path.
5. If r>A ∗ threshold, reject this path and return to step 3. Else, path is selected for the request.
6. If no path available, request rejected and network is congested.

Finally the wormhole attack will be detected and prevented in wireless sensor network.

## 4. SIMULATION AND RESULTS

To evaluate the above analysis, NS2 has been used for simulation. The network comprises of 30 homogeneous nodes.

Out of these nodes last node act as Base Station and one node as attacker node. Each node moves with constant speed. Some of the experimental parameters used in the simulation are listed in Table-2.

**Table-2.** Parameters in the Network Model.

| Parameters | Values |
|---|---|
| Initial energy | Eini 1 Joule per node |
| No. of ants | ( N) 3,5,7,10,12,15 times the neighboring nodes of source node |
| Packet size (K) | 1 K |
| Band width (B) | 1 Mbits/s |
| Traffic load | Random |

To evaluate the results we had varied the no. of ants at the source node as given in Table. It is clear that minimum number of ants can detect maximum number of routing attacks. It is observed that energy consumption at source node is directly proportional to number of ants generated.

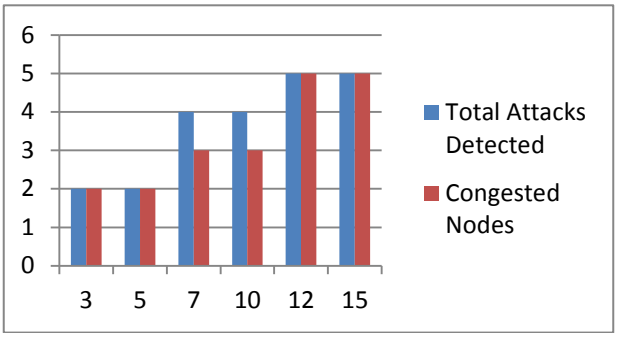



**Figure-1.** Average detection rate

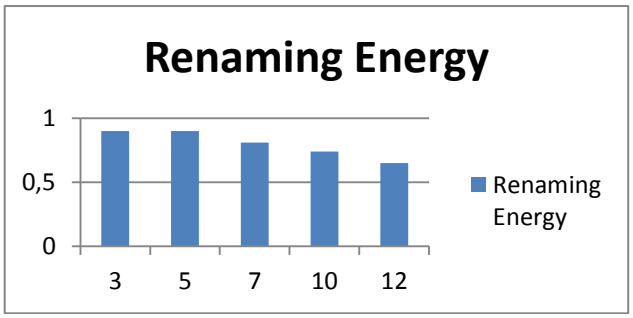



**Figure-2.** Energy consumption rate.

## 5. CONCLUSIONS AND FUTURE WORK

WSN is an emerging technology but they are prone to security threats, wormhole attacks and intrusion. This paper presented an ant based novel approach using swarm intelligence to detect anomalies.

The proposed approach will be tough challenge to attackers because of double monitoring. Simulation results show the efficiency of using ants for this purpose. In future detection of other types attacks using this algorithm may be attempted and more adaptive values for some more QoS Parameters can be explored.

## REFERENCES

[1] I.F Akyildiz, W.Su, Y. Sankarasubramaninam, E. Cayiric. “Wireless Sensor Networks: a Survey”. New York, NY, USA: Computer Networks: The International Journal of Computer and Telecommunications Networking, 2002.

[2] Xie Hui , Zhang Zhi-gang , Zhou Xue-guang , “A Novel Routing Protocol in Wireless Sensor Networks based on Ant Colony Optimization” International Conference on Environmental Science and Information Application Technology., 2009.

[3] Song Han, Elizabeth Chang, Li Gao and Tharam Dillon. "Taxonomy of Attacks on Wireless Sensor Networks". Springer London, 2006.

[4] Hemanta Kumar Kalita and Avijit Kar. "Wireless Sensor Network Security Analysis". International Journal of Next-Generation Networks (IJNGN), 2009.

[5] Karlof, C. and Wangner, D. "Secure Routing in Wireless Sensor Network Attacks and Countermeasures", In: proceeding of the 1st IEEE International Workshop on Sensor network Protocols and Applications, 2003

[6] Anthony D. Wood and John A. Stankovic. A Taxonomy for Denial- of – Service Attacks in Wireless Sensor Networks. CRC Press, 2005.

[7] Dimple Juneja, Neha Arora, Sandhya Bansal. "An Agent based Routing Algorithm for Detecting Attacks in Wireless Sensor Networks". IJCIR, 2010.

[8] Kennedy J, Shi Y. and Eberhart R.C., "Swarm Intelligence", Morgan Kaufmann Publishers, San Francisco, 2001.

[9] A. tiranuch, and W. Jie, "A survey on Intrusion Detcetion in Mobile Ad hoc Networks", Chapter 7, Wireless/Mobile Networks Security,Springer, 2006.

[10] Chong Eik Loo, Mun Young Ng, Christopher Leckie, Marimuthu Palaniswami. "Intrusion Detection for routing attacks in Sensor networks". International Journal of Distributed Sensor Networks, 2006.

[11] Bo Yu, Bin Xiao. "Detecting Selective Forwarding Attacks in Wireless Sensor Networks" .Greece: IPDPS, 2006.

[12] Bharat Bhargav, Weichao Wang. Visualization of Wormholes in Sensor Networks. New York, NY, USA: ACM press, 2004.

[13] Sumit Gupta, "Anomaly Detection in Wireless Sensor Networks ", MS Thesis, University of Houstan.

[14] J. Bruten, O.Holland and R.Schoonderwoerd, "Ant-like agents for load balancing in telecommunications networks" Agents'97 Marina delRey CA USA, 1997.

[15] Heng Chen, Depei Qian, Weiguo Wu, Lu Cheng, "Swarm Intelligence Based Energy Balance Routing for Wireless Sensor Networks" iita,Second International Symposium on Intelligent Information Technology Application., 2008.