Available online at www.sciencedirect.com

SciVerse ScienceDirect

Procedia Computer Science 10 (2012) 1010 – 1017

Procedia Computer Science

The 7th International Symposium on Intelligent System Techniques for Ad hoc and Wireless Sensor Networks (IST-AWSN).

Hidden Markov Model for shortest paths testing to detect a Wormhole Attack in a localized Wireless Sensor Network.

Victor Obado[1],Karim Djouani[2],Yskandary Hamam[3].

Department of Electrical Engineering/French South African Institute of Technology (FSATI),

Tshwane University of Technology, Private Bag X680 Pretoria 0001, South Africa.

Abstract

The wormhole attack is one of the most popular and serious attacks in Wireless sensor networks and most proposed protocols to defend against this attack use extra hardware which impacts highly on the cost of implementation as well causing extra overheads which have high implications on the sensors power consumption. Due to the limited resources in the sensor nodes, protocols developed for wireless sensor networks should not impact heavily on the computational overheads and power consumption in order to extend the network lifetime. In this paper, we exploit the Hidden Markov Model (HMM) Viterbi algorithm, to detect the wormhole attack based on the maximum probabilities computed for a hidden state transition. We use different shortest paths hop count costs between a source and a destination node as the states input to the Viterbi algorithm, earmarking the least cost paths as the suspect wormhole paths, for a given observation sequence of the given shortest paths.

Keywords: Underwater Sensor networks; Viterbi Algorithm; Hidden Markov Model; Wormhole Attack.

1. Introduction

A wireless sensor network(WSN) consists of a collection of wireless sensor nodes which exchange data among themselves without the reliance on a wired backbone network [1]. Sensor nodes are typically distinguished by their limited power, processing and memory resources. Their applications allow users to monitor, track, and observe a variety of objects and phenomena in different environments [1] . The WSNs can also be classified into five main categories: Terrestrial WSN, Mobile WSN, Underground WSN, Underwater WSN, and Multimedia WSN [1].

Sensing of coastal management and surveillance tasks, or ocean monitoring for disaster prevention and recovery applications can be supported by deployment of underwater sensor networks. Sink nodes are normally placed on the sea surface established as buoy to relay the information to the onshore station via

1877-0509 © 2012 Published by Elsevier Ltd. Open access under CC BY-NC-ND license.
doi:10.1016/j.procs.2012.06.140

satellite or long-range radio frequencies. The aquatic environments however have a major difference from its terrestrial counterparts in the shift from radio frequency to acoustics, that changes the speed of communication from that of light to that of sound [2] .
Information routing in these networks faces a number of security threats. One such threat is the wormhole attack [3] . Since the sensors use a shared acoustic channel to send information in underwater environments, the malicious nodes can eavesdrop on the packets, by capturing packets from one location and "tunneling" these packets to the other malicious node, which is assumed to be located at some distance. The second malicious node is then expected to replay the "tunneled" packets locally. This attack takes place using either in-band (tunneling) or out-of-band communication to transfer the packets between these locations. This can give nodes that are in the neighborhood of the attackers the impression that links exist between them and other nodes that are in reality far outside of transmission range, severely disrupting communication and/or the localization process. Moreover it is possible even if the attacker has not compromised any hosts and even if all communication provide authenticity and confidentiality. An example of a wormhole attack is illustrated in the figure below:

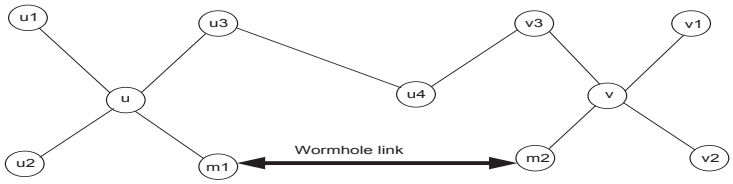

Figure1: Wormhole link between a pair of nodes u and v fabricates a fake connection between them.

This paper focuses on a detection approach based on the computationally efficient Viterbi algorithm that enables us to utilize the shortest paths hop count costs between a source node and destination node in the network as states, to compute the hidden state sequences using the maximum state transition probabilities, for a given observation sequence of the shortest paths. This paper is organized as follows: in section two we discuss the related works that have been done, in section three we present our system model, in section four we discuss the simulation results then finally in section five we conclude our work.

1.1. Related Work.

Bhargava et al [8], proposes a detection approach based on localization of nodes using the Multi Dimensional Scaling (MDS) technique of localization, enabling comparison to be made on the structure of the network with and without the attack. By detecting the anomalies introduced by the fake connections, the attack is detected. It however, like many MDS techniques has a problem of scalability since it relies on a central processing node for all the computations. Wang et al Presents a similar approach in [9] but takes into account the existence of more than one wormhole threat and is also robust against distance estimation errors. [10] on the other hand concentrates on the underwater scenario. He uses ToA based technique to measure the distances between the sensor nodes, which requires hardware components for timing, hence is undesirable since it has a high implication on cost. MDS on the other hand concentrates more on the general layout of the network and not the nodes position accuracy. Marco Pugliese 2008 [6] used a non parametric version of HMM, the Weak Process Model (WPM), wherein state transition probabilities are reduced to rules of reach ability to detect anomalies in a network, where he detected the wormhole attack based on identified observable events correlated to a threat by applying a set of anomaly rules to the incoming traffic. Alarms were then issued as soon as one or more high potential attacks were detected. Guofei Jiang [7] analyzed the properties of such weak process models and proposed a recursive algorithm to compute the hypotheses of the hidden state sequence and the size of the hypothesis set, for a robust process detection. These works did not take into account the exact probability values for the state transitions and observational probabilities since they set for such probabilities, binary

(0,1) values depending on whether the values were close to 1 or 0, which could compromise on the detection accuracy. Our approach uses exact probability values and RSS for distance measurement which does not require any extra hardware, and proceeds to exploit the Viterbi algorithm to compute maximum hidden state transition probabilities for its detection, given a HMM model.

1.2. System Model

A. Distance measurement derivation

To calculate the distance we need to know the values of the RSSIs from the beacon nodes to the sensor node. This value can be obtained by taking into account the absorption attenuation of the signals from the beacon node to the sensor node, denoted as α. Thorp model[11] is used to calculate the value of α, given the frequency, as follows:

$$\alpha = 1.0936[0.1(\frac{f^2}{1+f^2}) + 40(\frac{f^2}{4100+f^2})] \quad (1)$$

Firstly, we considered the spherical spread loss[12] since it provides a reasonable fit to the measured data under a wide variety of conditions. Consequently, the RSS can be calculated based on the following equation.

$$RSS = TLsph + \alpha\, dist \times 10^{-3} \quad (2)$$

Where $TLsph$:denotes the spherical spread loss and equals $20log10(R)$,
R :denotes the distance the acoustic wave has travelled,
α :denotes the thorp attenuation model [4].
The next step is to solve Equation (2) based on Dist variable. Lambert W function is manipulated for extracting the inverse of Equation (2), as it is an exponential function [4], to derive the final distance equation,

$$Dist = \frac{20000W(\frac{\ln(10)\alpha e^{\frac{\ln(10)}{20}} \times RSS}{20000})}{\alpha \ln(10)} \quad (3)$$

since $ln(10) =$ 2.30258509 and α=1.1498,

$$Dist = 7554.26129654 \times W(1.32327 \times 10^{-4} \times e^{0.115129255 \times RSS}) \quad (4)$$

Hosseini et al, [4] proved that the underwater RSS based distance measurement can be an application of the Lambert W function. Equation (4) represents the final equation of Distance based on RSS via Lambert W function, according to Hosseini et al [4] , who also carried out a Lambert W function proof to prove the accuracy of the computed distances.

C. Shortest Paths Computation

Given a localized network [13-15], the distance measurements between the network nodes and the maximum transmission range r, the neighboring nodes are connected through arcs.

Let (N,A) be a network with N nodes and m arcs, where any (i, j) ∈ A is assigned with the value $c_{ij} \in R$, that denotes the cost, or distance of (i, j).
A path p from i ∈ N to j ∈ N in (N,A) is a sequence of the form p = (i = v1, v2, . . . , j = vℓ(p)), where (v_k, v_{k+1}) ∈ A, for any k ∈ {1, . . . , ℓ(p)−1}.
Here ℓ(p) is called the length of p, that is, its number of nodes, while i and j are called the initial and terminal nodes of path p, respectively. The total cost, or distance, of p is defined by:

$$C(p) = \sum_{u,v \in P} C(u,v) \tag{5}$$

Given x and y two nodes of p, $sub_p(x, y)$ represents its subpath from x to y. A path is said to be loop less when it has no repeated nodes. The set of loop less paths from i to j in (N,A) will be denoted by $P_{i,j}$, and given an initial, s, and a terminal, t, nodes (s not equal t), then P will be used for $P_{s,t}$. The concatenation of p ∈ $P_{i,j}$, q ∈ $P_{j,\ell}$, denoted by p ⋄ q, is the path from i to ℓ formed by path p followed by q.
Given K ∈ N, in the K shortest loop less paths problem is intended to compute loop less paths $p_1, \ldots, p_K$ from s to t in (N,A), by non-decreasing order of the cost such that;
$c(p_1) \leq \ldots \leq c(p_k)$ and
$c(p_k) \leq c(p)$, for any $p \in P - \{p_1, \ldots, p_K\}$.
Assuming the k shortest loop less path has the form;
$p_k = (v_1 = s, \ldots, v_{\ell(pk)} = t)$, *for* $k = 1, \ldots, K$.
Yen's proposal [10] to obtain new candidates is to partition the set of loop less paths in the following way:

$$P - \{p1\} = \bigcup_{i=1}^{l(p1)} P^i(v_i), \tag{6}$$

$$P^j(v_{d(pk)}) - \{pk\} = \bigcup_{i=d(pk)}^{l(pk)} P^k(v_i), \qquad k > 1 \tag{7}$$

where $P^j(v_i)$ denotes the set of the loop less paths, different from $p_1, \ldots, p_j$, that have sub_{pj} (s, v_i) as the initial sub path, common with path p_j , for some $1 \leq j < k$. When a p_k is picked up in X the set $P^j(v_{d(pk)})$ where p_k was determined is considered, which means that it is partitioned by computing the shortest loop less path in each of the subsets. Yen noted that the best deviation from p_k at node v_i is sub_{pk} (s, vi) ⋄ q_i, where q_i is the shortest path from v_i to t, when the nodes $v_1, \ldots, v_{i-1}$ and the arcs (v_i, x) ∈ $\{p_1, \ldots, p_k\}$ are removed from the network. The loop less path p_k is called the father of the new candidates determined (known as p_k deviations) and $v_{d(pk)}$ the deviation node of p_k. Thus, analyzing a given p_k consists of modifying (N,A), by deleting some arcs and some nodes, and solving a shortest path problem between a pair of nodes.

D. Normal behavior modeling

In this paper, we use HMM to model the wormhole attack detection approach.
HMM was applied to model the sequence of shortest paths decisions made by a source node to communicate to a destination node, because it is very useful for modeling the sequence information [16].
An HMM λ is described as $\lambda = (A, B, \Pi)$. An HMM is characterized by a set of states S, a set of possible observation symbols V, a number of observation symbols M, state transition probability distribution A, observation symbol probability B and initial state distribution Π [16]. The set of all shortest paths hop count costs corresponds to the set of states, while the set of all the shortest paths corresponds to that of possible symbol observations V, and a number of the shortest paths decisions taken by the source node correspond to M, for a length of an observation sequence time T.

This phase is to model the normal behavior, which determines HMM parameters for the computation of the maximum state transition probabilities via the Viterbi algorithm.

E. Viterbi algorithm for wormhole attack detection

We applied the Viterbi algorithm to find optimal state sequence, given the sequence of observation symbols M, for a given sequence time, T. The computed state sequence is based on the maximum probabilities computed at each sequence step to determine which state is encountered at that given step.
In our detection approach, since the set of states corresponds to the shortest paths hop count costs, and we know that the wormhole attack advertises the best path with the least cost, we ear marked all the least cost states in the computed state sequence to be the suspect costs advertised by the wormhole path, and compared their maximum transition probabilities at each of the respective sequence steps of occurrence, with highest probability value depicting the highest likeliness that the particular cost was being advertised by a wormhole path.
The procedures of the Viterbi algorithm are as follows:
Initialization:
$\delta_1(i) = \Pi_i b_i(O_1), \quad 1 \le i \le S$
$\alpha_1(i) = 0$

$\delta_1(i)$ is the probability that symbol O_1 occurs at time $t=1$ at state i. The variable $\alpha_1(i)$ stores the optimal costs states.
Recursion:
$\delta_t(j) = max[\delta_{t-1}(i)a_{ij}]b_j(O_t), \quad 1 \le i \le S \quad 2 \le t \le T \text{ and } 1 \le j \le S$
$\alpha_t(j) = argmax[\delta_{t-1}(i)a_{ij}], \quad 1 \le i \le S \quad 2 \le t \le T \text{ and } 1 \le j \le S$
$\delta_t(j)$ denotes the weight accumulated when we are in state j at time t as the algorithm proceeds. The argmax operator selects the index j which maximizes the bracketed expression, to obtain the sequences of the hidden states.
Termination:
$P^* = max[\delta_T(i)] \quad 1 \le i \le S$
$q^*_T = argmax[\delta_T(i)] \quad 1 \le i \le S$

1.3. Simulation tests and results

It is necessary for each new designed or developed algorithm, mechanism, or protocol, to be evaluated and tested to demonstrate its integrity. Therefore, a simulation scenario has been established for validating the developed detection approach.

A. Shortest paths simulation

Using the accurate distance measurements [4], the maximum transmission distances, r=40m, and a localized 400m by 400m network, we simulated four shortest paths between a single source node and destination node, using MATLAB. In addition, the simulation results of the distance measurements results[4] showed steady values with minimal errors as shown in the sample table below:

Actual distances	Lambert distances	Error
296.4675	296.3628	0.1047
213.0376	212.9615	0.0761
395.2025	395.0646	0.1379

Table 1: Table comparing the actual distances and Lambert computed distances

The results of the shortest paths, marked by the red paths in the localized network between a single source node 37 and destination node 10 is shown in the graph in the next page, with the 4 shortest paths having hop count costs according to the paths taken, as also shown below:
Cost 1= 5 hop counts (37-2-21-27-7-10)
Cost 2= 5 hop counts (37-21-27-1-7-10)
Cost 3= 4 hop counts (37- 21- 27- 7-10)
Cost 4= 5 hop counts (37-21-27-1-12-10)

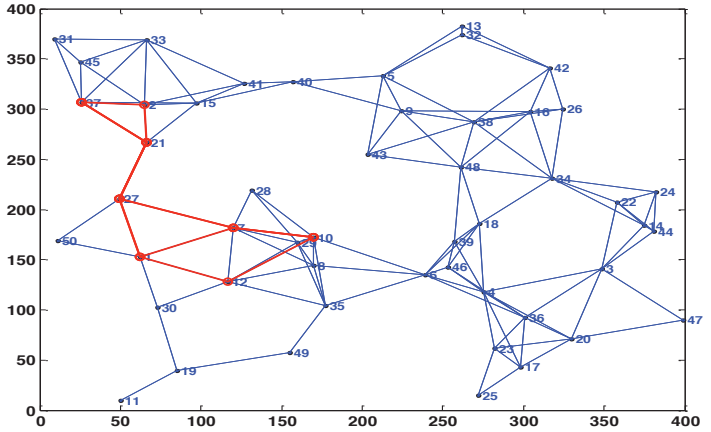

Figure 2: The network graph depicting the localized network with a 40m neighbour relationship on a 400m by 400 m field.

B. HMM Viterbi Wormhole detection approach

After successfully simulating the shortest paths problem, we ran a random observation sequence steps, O for time T =10, where each entity in the observation sequence array depicts the random path decision made at that particular time step.
O = [3 1 4 1 2 2 2 1 4 3]

For example in our array, at time t=1 the random path decision made was a path number 3 meaning the hidden state computed for this sequence step is the cost of this random path 3. If another sequence step has the same random path decision, in our case t=1 and t=3, the computed hidden state would normally be different from any other same random path decision. This means that for each step an independent random decision is made for what the computed hidden state will belong to the random path decision at time t. so it would occur that the same path decisions in the array would not have the same value of path costs. With the set of states, S= {cost 1,cost 2, cost 3, cost 4} and the set of observations, V={path 1, path 2, path 3, path 4}, to simulate the hidden state sequences, and their respective maximum probabilities at each sequence time step, t, given the HMM model λ=(A,B,Π), Where A is the $S \times S$ state transition matrix, B is the $V \times S$ observation matrix and Π is a uniform initial S state distribution probability.
Since the wormhole path advertises the best path with the least cost, we set all the path costs greater than the minimum costs in the computed hidden state sequence to a probability of zero(0), depicting zero possibility of the path being a wormhole path. Since the wormhole attack advertises the least costs paths in a network, we considered the maximum probabilities for all the least costs states in the computed state

sequence. Our simulation results showed the computed probabilities and plotted them against the sequence time steps, t.

A threshold probability of 0.5 was set for the detection process. If at a time sequence step the probability of the hidden least cost state is higher than the threshold, an alarm is raised at this particular sequence step, to depict the existence of the wormhole attack. Necessary measures can then be taken to avoid this route, at such a particular time sequence that an alarm is raised. Our simulation generated the computed hidden states, δ as shown below, for a random observational sequence steps for a total of time, T=10. Recall that cost 1=5 hops, cost 2=5 hops, cost 3=4 hops and cost 4=5 hops.

Hidden states, δ = {cost 3, cost 3, cost 4, cost 1, cost 4, cost 2, cost 1, cost 1, cost 4, cost 2}.

The graph shows the detection results, for a random observational sequence steps for a total of time, T=10.

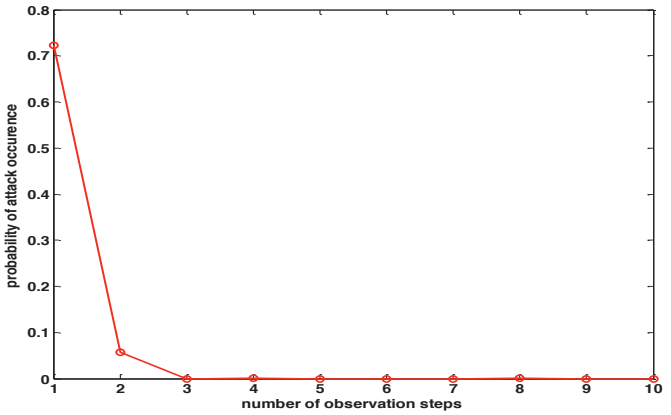

Figure 3: Graph depicting the probability level of an attack occurring at each observational step.

From the graph, at the observation sequence step t=1, a random path decision of path 3 was made and for this path, the hidden state is cost=4 hops, which is the least cost meaning the path decision could be a wormhole path. Same applies to step t=2 since the hidden state for the random path 1 decision is also a cost of 4 hops.

Since we plotted maximum transition probabilities of the hidden least costs states at each step t as they depict the wormhole attack, we tested the likelihood of the path decisions at t=1 and t=2 being a wormhole path.

Since at t=1 the probability is greater than the threshold 0.5., the path 3 decision was a wormhole path and an alarm generation was made to stop communication.

At step t=2 the probability is less than the threshold hence depicts a safe route. No alarm generation was necessary and the path 1 decision was a safe path.

The rest of the sequence steps show zero probability of the path decisions being a wormhole path since the computed hidden states were not the least path cost, that is were greater than 4 hops.

1.4. Conclusion

In this paper we successfully exploited the Viterbi algorithm approach and Lambert W function, as shown in the simulation results, for the detection of the wormhole attack and accurate inter node distance computation. Our approach was attractive as the recursive nature of the Viterbi algorithm would limit computational overheads and hence reduce power consumption of the resource constrained sensors nodes.

REFERENCES

[1] J. Yick, Mukherjee, B. and Ghosal, D., "Wireless sensor network survey," *Computer Networks.*, vol. 52(12), pp. 2292 – 2330., 2008.

[2] J. Heidemann, Ye, W., Wills, J., Syed, A. and Li, Y., "Research challenges and applications for underwater sensor networking," *IEEE Wireless Communications and Networking Conference*, vol. vol. 1., pp. 228 – 235., 2006.

[3] J. K. Weichao Wang, Bharat Bhargava,Mario Gerla, "Visualisation of wormholes in underwater sensor networks: a distributed approach," *Int. J. Security and Networks,*, vol. Vol. 3, pp. 10-23, 2008.

[4] M. C. Hosseini, H.; Chai Kok Soon; Budiarto, R, "RSS-based distance measurement in Underwater Acoustic Sensor Networks: An application of the Lambert W function," in *Signal Processing and Communication Systems (ICSPCS), 2010 4th International Conference* 2010, pp. 1-4..

[5] J. Yen, "Finding the Lengths of All Shortest Paths in N-Node Nonnegative-Distance Complete Networks Using ~N 3 Additions and N 3 Comparisons," University of Santa Clara, Santa Clara, California, 1970.

[6] G. A. Pugliese M., Santucci F., "A Weak Process Approach to Anomaly Detection in Wireless Sensor Networks," EU FP6 NoE HYCON, 2008, pp. 1-7.

[7] G. JIANG, "Robust Process Detection Using Nonparametric Weak Models," *INTERNATIONAL JOURNAL OF INTELLIGENT CONTROL AND SYSTEMS*, vol. 10, pp. 33-42, MARCH 2005 2005.

[8] W. W. B. Bhargava, "Visualization of wormholes in sensor networks," in *WiSe'04,* , C. a. D. o. C. S. P. University, Ed. Philadelphia, Pennsylvania, USA, 2004, pp. 51-60.

[9] A. L. Weichao Wang, "Interactive Wormhole Detection in Large Scale Wireless Networks," in *IEEE Symposium on Visual Analytics Science and Technology* Baltimore, MD, USA: IEEE, 2006, pp. 99-106.

[10] K. J. W. Weichao, B. Bharat and G. Mario, "Visualisation of wormholes in underwater sensor networks: a distributed approach," in *Int. J. Security and Networks,*. vol. 3: Inderscience Enterprises Ltd, 2008, pp. 10-23.

[11] W. H. Thorp, "Analytic Description of the Low-Frequency Attenuation Coefficient.," *Acoustical Society of America Journal*, vol. 42, p. 270, 1967.

[12] R. J. Urick, "Principles of Underwater Sound(3rd ed.)." vol. 1: Penisula Publishing, 1983.

[13] V. Chandrasekhar, Seah, W. K., Choo, Y. S. and Ee, H. V., "Localization in underwater sensor networks - Survey and challenges," in *WUWNet 2006 - Proceedings of the First ACM International Workshop on Underwater Networks*, 2006, pp. 33 – 40.

[14] T. Hui, Shuang, W. and Huaiyao, X., "Localization using Cooperative AOA Approach.," in *Wireless Communications, Networking and Mobile Computing, WiCom 2007*, 2007, pp. 2416–2419.

[15] K. H. Lee, Yu, C. H., Choi, J.W. and Seo, Y. B., "ToA based sensor localization in underwater wireless sensor networks," in *Proceedings of the SICE Annual Conference*, 2008, pp. 1357 – 1361.

[16] L. Rabiner, "A tutorial on Hidden Markov Models and selected applications in speech recognition," *IEEE* vol. 77, pp. 257-286, February 1989.

Victor Obado received his BSc. in Computer Science in 2008 from Masinde Muliro University, Kenya. He is currently pursuing MTech. Electrical Engineering at French South African Institute of Technology (F'SATI)/Tshwane University of Technology, South Africa. His research interests are in the area of wormhole attack detection in underwater sensor networks.