A Reputation-Based Method for Detection of Attacks in Virtual Coordinate Based Wireless Sensor Networks

Divyanka Bose
Department of Electrical and Computer Engineering
Colorado State University
Fort Collins, CO 80523, USA

Anura P. Jayasumana
Department of Electrical and Computer Engineering
Colorado State University
Fort Collins, CO 80523, USA

***Abstract*—Virtual Coordinate (VC) based Wireless Sensor Networks (WSNs) are susceptible to attacks resulting from malicious modification of VCs of individual nodes. While the impact of some such attacks is localized, others such as coordinate deflation and wormholes (tunneling) can cause severe disruptions. A comprehensive solution for detection of such attacks is presented that combines Beta Reputation System and a reputation based routing scheme. Latter ensures safe communication that bypasses malicious nodes during detection process. Attacks are identified by detecting changes in shape of network using topology maps. The topology distortion is rated using clusters identifiable by existing VCs thus requiring low computation and communication overhead. Simulation based evaluations demonstrate that the scheme efficiently detects deflation and wormhole attacks. The detection scheme easily differentiates between the changes in the network due to node failures, e.g., caused by battery drain, from those due to an attack.**

Keywords- Trust Model, Beta Reputation, Wireless Sensor Networks, Topology Maps, Security, Virtual Coordinates

I. Introduction

Vast majority of algorithms essential for WSNs, such as those for self-organization, routing, topology control, boundary detection, and event detection depend on a coordinate system. Virtual Coordinate (VC) based WSNs [1][2] depend on the connectivity and topology of the network. The VCs of a node corresponds to shortest hop distances from the node to a subset of nodes, called *anchors* or *landmarks*. VC system possesses numerous advantages over physical coordinate based systems in terms of cost, robustness and scalability for large-scale networks as well as those deployed in harsh environments [3].

The VC based algorithms, such as routing [1][2][4] rely on the correctness of the VCs of the nodes. As a consequence, VC based systems are highly susceptible to various types of malicious attacks that modify the VCs. Our work focuses on the attacks which aim to disrupt the network, e.g., cause mis-routing and packet timeout, by modifying VCs [5]. Now, we take a closer look on two types of attacks namely, Coordinate Deflation and Wormhole.

Coordinate Deflation attack [6] is caused by taking a legitimate node under the control of an attacker and falsely claiming and propagating lower VC values for the attacked node. The neighbors of this node then assign incorrect VC for themselves due to lower perceived distance through the attacked node. Another destructive attack is the wormhole/tunneling [6]. WSNs use radio channels for communication. Thus, those nodes which are within a node's radio range, are considered as it's neighbors with a hop distance of 1. Wormhole attacker generates strong radio/physical channel between two nodes that are actually not near to each other, thus creating a tunnel. Thus, more packets are routed through the wormhole as they provide a shorter hop count. Thus, sensitive data may be compromised due to malicious listeners of the wormhole.

Attack detection itself can be hindered by the compromised nodes, e.g., by interfering with packets used for detection. Thus, first we present a reputation scheme for nodes based on the Beta Reputation System [7] triggered by change of coordinates of a neighbor node, and a trust based routing method for VC based WSNs. Higher the reputation of a neighbor, higher is the nodes trust to send high reliability packets through that neighbor. Second, we introduce a novel detection technique to detect an attack which uses the Topology Preserving Maps (TPM)s [3]. TPMs are capable of capturing layout and topology features from VCs. The changes that occur in the topology due to an attack is captured in the detection scheme. We demonstrate through simulation results that, the detection scheme is highly efficient in differentiating changes in the network due to attacks from those due to changes such as fading or node shut-down due to battery drain causing missing nodes.

II. Reputation System for VC based WSNs

In this section, we present a reputation system based on The Beta Reputation System [7] to characterize the trust value of the nodes. The Beta Reputation System takes integer values of positive and negative feedback as input. Consider an entity *x*, which gives a reputation value to another entity *t*. If the positive feedback given by *x* to *t* is r_t^x and the negative feedback given is s_t^x, then the reputation rating, $Rep(r_t^x, s_t^x)$

978-1-4673-6770-7/15/$31.00 ©2015 IEEE

[7] using the expected value of the Beta Distribution function is expressed as

$$Rep(r_t^x, s_t^x) = \frac{r_t^x}{r_t^x + s_t^x} \tag{1}$$

The implementation of Equation 1 to VC based WSNs is now explained. Let node *j* be a neighbor of node *i*. Firstly, we calculate the feedback values given by the neighbor nodes. If node *j* is attacked, its changed VCs are broadcasted to node *i*. The positive feedback given by *i* to *j*, r_j^i is the number of VCs that are equal. The negative feedback, s_j^i is the difference in original VC values and the changed VC values.

The calculation of positive and negative feedback is explained using an example. At the initial setup of the network, each node initializes the reputation of its neighbor nodes as 1. Consider a node A which has its neighbor reputation as (N_1:1, N_2:1, N_3:1, N_4:1), which is $(Neighbor : NeighborReputation)$. Let the original VCs of the node N_4 be [6, 3, 5, 2]. Consider a Coordinate Deflation attack on node N_4 which broadcasts the new VCs of node N_4 as [1, 1, 1, 2]. Node A receives the changed VCs of node N_4. The $r_{N_4}^A$ value given by node A to N_4 is 1, since only 1 element among all VCs of N_4 has not changed. The $s_{N_4}^A$ value is 11 which is the sum of the difference of the VC elements, $(6-1)+(3-1)+(5-1)$.

The Reputation Rating of node *j* by node *i* is calculated using Equation 1. For the example network, the Reputation Rating $Rep_{N_4}^A$ is $\frac{1}{1+11} = 0.08$. The neighbor reputation database of node A is now updated to (N_1:1, N_2:1, N_3:1, N_4:0.08). The VC of node A are updated as required due to the changes in VC of node N_4. The updated VC of node A further propagates to others and similarly each node's neighbor reputation in the entire network gets updated. This reputation system ensures that during communication of high reliability packets, node A sends its data via a neighbor node other than N_4, as it has the lowest reputation.

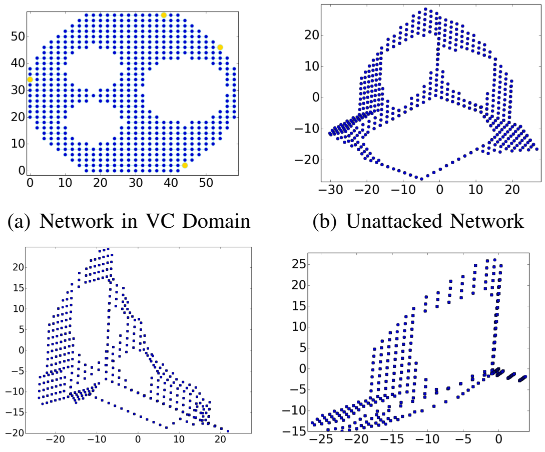
III. Topological Changes in the network

Topology Preserving Maps (TPMs) [3] capture the topological information of a network concisely, and provide layout maps that capture information about physical layout, shapes and features of 2-D and 3-D sensor networks. TPMs are derived from the VCs via a partial Singular Value Decomposition(SVD) [3]. Consider a network with *N* nodes and *M* anchor nodes. Let the VC of node *i* be denoted as $[i_0, i_1...i_M]$, where $i_0, i_1...i_M$ correspond to the distance to each of the M anchors. Let P be the *NxM* matrix with the *i*th row being the *M-length* VC of node *i*. SVD is applied on matrix P that generates *U, S* and *V* matrices. Then the projection of P onto V is

$$P_{SVD} = P.V \tag{2}$$

$V^{(j)}$ is denoted as the j^{th} basis column of V. Then the topological coordinates of node i, (x_T^i, y_T^i) is described as

$$(x_T^i, y_T^i) = ([i_0, i_1...i_M].V^{(2)}, [i_0, i_1...i_M].V^{(3)}) \tag{3}$$



(a) Network in VC Domain (b) Unattacked Network

(c) Wormhole (d) Coordinate Deflation

Fig. 1. Topological Changes in Circular Network with Voids

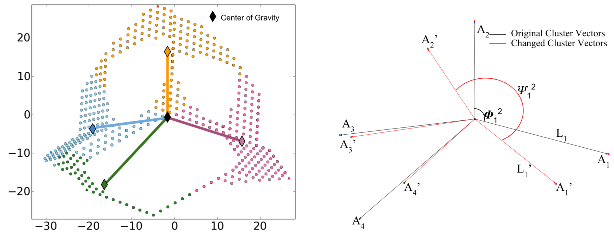
A computationally efficient approach that uses only a small subset of rows of P is described in [3]. The TPMs regenerate the original topological features of the network, such as voids and edges. It also recovers directional relationships that are lost in the VC representation. The anchor selection for the network is done using the Extreme Node Search (ENS) Algorithm [8]. The ENS algorithm attempts to choose the anchor nodes which are farthest apart and those which are the corner nodes of the network.

Next we discuss the topological changes that occur in the network due to an attack. Consider the Circular network with voids [9] shown in Figure 1(a). Figure 1(b) shows the topological map of this network. Figure 1(c) shows the changed topological map due to a wormhole attack. Figure 1(d) shows the affected TPM after coordinate deflation attack. The drastic changes in the topological maps of the pre-attack and post-attack networks are visually seen in Figure 1. Wormhole causes the topological map to fold over and Coordinate Deflation causes the topological map to converge towards the attacked node. Thus, the change in shape of the TPMs can be used to successfully detect an attack on VCs of the network.

IV. TPM based Detection of an Attack on the Network

The neighborhood of the attacked node is most affected as VCs of nodes are updated by observing neighbor's VCs. If a neighbor provides shorter hop count to the anchor nodes, i.e., deflated VCs, the nodes update their VCs accordingly. Thus, the topology coordinates of that region will be distorted the most. Thus, the network is divided into clusters to capture this change in the neighborhood of the attack. Although clustering can be carried out in different ways, here we assign clusters around anchors, with each node assigned to the cluster of that anchor node to which it is closest to. Clustering of the network gives the advantage of localizing the attack to a subset region of the network.

The clustered topology map of the Circular network is



(a) TPM of Clustered Network (b) Original vs Changed CGs

Fig. 2. Circular Network with Anchor-based Clusters Identified

TABLE I
NOMENCLATURE FOR DETECTION SCHEME

Nomenclature	Description
M	Number of Anchor Nodes
A_i	i^{th} anchor node, $1 \leq i \leq M$
A_j, A_k	Adjacent cluster neighbors for A_i
ϕ_i^j, ϕ_i^k	Original Adjacent angles with adjacent neighbors
θ_i^j, θ_i^k	Changed Adjacent angles with adjacent neighbors
L_i	Length of original i^{th} cluster vector
L_i'	Length of changed i^{th} cluster vector

shown in Figure 2(a). To find the change in topology shape, we use the Center of Gravity (CG) or mean *(x,y)* position of each cluster and of the entire network as shown in Figure 1(c). Reference values for these are computed during the initial stage when the network is assumed to be in perfect conditions. The CG of the entire network is referred as the Network CG and the CGs of the clusters are referred to as the respective anchor node's Cluster CGs.

For detecting an attack, the change in position of the CG is needed with respect to itself and with respect to its adjacent cluster CGs. To achieve this, we use the angle between two adjacent cluster CGs and the distance of the Cluster CGs to the Network CG. The connecting line from the Cluster CG to the Network CG is defined as the Cluster Vector. Visually, the adjacent cluster CGs for any single cluster can be easily determined. However, to find the adjacent topological neighbors for a cluster systematically, we use the angle of the cluster vectors to the X-axis. These angles are calculated between $0 - 2\pi$ anti-clockwise from the X-axis. The closest two cluster CGs are chosen as the Adjacent Cluster Neighbors.

The Circular network is mounted with a wormhole attack. The nomenclature for the detection scheme algorithm is tabulated in Table I. ϕ_i^j, ϕ_i^k and L_i are calculated at the time of network setup. In Figure 2(b), cluster vector A_1 maintains ϕ_1^2 and ϕ_1^4 with cluster vector A_2 and A_4. After the network suffers a change in the VCs of the nodes in the network, the CG of the clusters are recalculated as per the changed VCs. A_1', θ_1^2 and θ_1^4 are calculated.

We define two terms, *Detection Rating D* and the *Threshold Value T*. The value of D provides a rating for the entire network using both the difference in ϕ and θ, and the difference in length of the cluster vectors of each cluster. T is the threshold value that is set, above which the network is declared under attack and below which the change in topology is considered legitimate. The computation of D is explained in Algorithm 1.

Algorithm 1 Algorithm to calculate Detection Rating

```
Angle rating for cluster $i$    $\gamma_i = \frac{\frac{|\phi_j - \theta_j|}{\phi_j} + \frac{|\phi_k - \theta_k|}{\phi_k}}{2}$
Length rating for cluster $i$    $L_i = \frac{|l_i - l_i'|}{l_i}$
Cluster rating $C_i = \gamma_i + L_i$
Detection Rating $D = \frac{\sum_{i=1}^{M} C_i}{M}$
```

The value of D returned by Algorithm 1 is compared to threshold value *T*. If $D > T$, then it is considered as an attack. If $D < T$ then it is considered as a legitimate change in the network. We show in the next section that, by choosing a proper threshold T, we can correctly detect an attack versus an environmental change in the network.

V. Results

Extensive results on the performance of the TPM based detection scheme is presented for the network shown in Figure 1. Enhanced results for other benchmark networks can be found in [10]. The network is subjected to 30 random coordinate deflation attacks and 30 random wormhole attacks, one at a time. We consider only one attack occurring at a time. To evaluate the robustness of detection scheme against node deaths, which routinely happen in networks, we also subject the network to 30 random node deaths of varying intensity. The detection rating for each kind of attack is plotted in Figure 3. The X-axis shows the experiment index and the Y-axis shows the value D. As seen in Figure 3, the detection ratings due to coordinate deflation attacks and wormholes lie in the range of 0.2 to 1.2 and the detection rating due to node deaths is in the range of 0.001 to 0.1. This demonstrates the existence of a threshold for discrimination between node deaths and attacks. For the remainder of the analysis, we set the threshold T to 0.1.

Correct Detection is defined as the value $D > T$ for attacks and $D < T$ for node deaths. *Non detection* is defined as the network being attacked but has not been detected by the detection scheme, i.e., $D < T$ for attacks. Non detections are seen when the attack causes very few VCs to change in the network, and in effect these have negligible or very minor affect. *False positive* is defined as a node death being declared as an attack i.e $D > T$ for node deaths. Existence of a node whose removal or death causes separation of two regions of the network, may cause drastic topological changes in the network. Such a change may be detected as an attack and results in false positives. If such a false positive need to be avoided, it is possible to implement a mechanism in which a node provides a warning to its neighbors when its power is critically low and is about to die, and propagating this information for remedial action such as issuing a warning or re-configuring the network.

The Correct Detection, False Positive and Non Detection rates are shown in Table II for the benchmark networks in [9] for $T = 0.1$. It is observed that the detection scheme is very

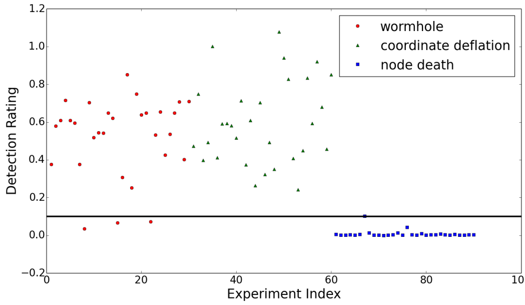


Fig. 3. Detection Rating

TABLE II
RESULTS FOR DETECTION SCHEME FOR VARIOUS NETWORKS

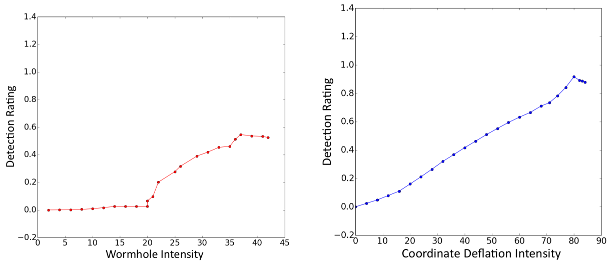
Type of Network		T=0.1	
	Correct Detection	False Positive	Non Detection
Block (550 nodes)	100%	0%	0%
Circular with Voids (575 nodes)	94.44%	1.11%	4.44%
M-Shaped (625 nodes)	100%	0%	0%
Building (350 nodes)	71.4%	28.6%	0.0%

efficient for all networks other than the Building network [10]. For the Building network, there are many critical nodes due to which the shape of the topology map will change due to any legitimate change in the VC of a single node. Thus, we get higher false positives due to drastic changes to the topology caused by node deaths.

Thus we can deduce that the algorithm performs exceptionally well when node density is high, i.e., each node has a high number of neighbors. The algorithm cannot differentiate between an attack and a node death for lower network density. If however, proper node death handling mechanisms are put in place, the detection scheme can be applied to sparse networks.

The distortion in the topology map due to an attack is also dependent on the intensity of an attack. Most often, when the attack does not create enough distortion in the topology map, the algorithm will fail to detect the attack. We now present the Detection Rating results for the varying intensity of attack.

In Figure 4(a), the X-axis shows the intensity of the wormhole attack, i.e., the number of hop counts before the wormhole between the two attacked nodes. Figure 4(b) shows the Detection Rating for varying intensity of Coordinate Deflation attack. For Deflation attack, the intensity is defined as the integer value by which the VCs of the attacked node has been modified. As seen in the plot, the Detection Rating increases as the intensity increases. We direct the readers to [10] for extended results on this scheme.



(a) Wormhole (b) Coordinate Deflation

Fig. 4. Attack Intensity vs Detection Rating Results

VI. CONCLUSION

A reputation based technique was developed for detection and localization of coordinate attacks in Virtual Coordinate based sensor networks. Since each node computes on its own the reputation value for other nodes, attackers cannot enforce better reputation for itself to other nodes. The reputation system is completely distributed and no central server is needed to maintain the reputation of the network. Results for the TPM based detection scheme shows that a robust Threshold Value T exists and that this approach is highly successful in detecting attacks. Also the scheme is successful in differentiating an attack from node death. The node deaths producing false positives as attacks are those that correspond to events that drastically change the topology, and hence are necessary for proper operation of the network. Also presented was a simple mechanism to eliminate false positives if necessary. A low-overhead method for localization of attack using VC-based clusters was presented. The novel TPM-based attack detection combined with the reputation based routing provides a better approach at tackling Virtual Coordinate based attacks.

REFERENCES

[1] Q. Cao and T. Abdelzaher, “A scalable logical coordinates framework for routing in wireless sensor networks,” in *Real-Time Systems Symposium, 2004. Proceedings. 25th IEEE International*, Dec 2004, pp. 349–358.

[2] M.-J. Tsai, H.-Y. Yang, B.-H. Liu, and W.-Q. Huang, “Virtual-coordinate-based delivery-guaranteed routing protocol in wireless sensor networks,” *Networking, IEEE/ACM Transactions on*, vol. 17, no. 4, pp. 1228–1241, Aug 2009.

[3] D. C. Dhanapala and A. P. Jayasumana, “Topology preserving maps: Extracting layout maps of wireless sensor networks from virtual coordinates,” *IEEE/ACM Trans. Netw.*, vol. 22, no. 3, pp. 784–797, Jun. 2014. [Online]. Available: http://dx.doi.org/10.1109/TNET.2013.2263254

[4] D. Dhanapala and A. Jayasumana, “Geo-logical routing in wireless sensor networks,” in *Sensor, Mesh and Ad Hoc Communications and Networks (SECON), 2011 8th Annual IEEE Communications Society Conference on*, June 2011, pp. 305–313.

[5] X. Du and H.-H. Chen, “Security in wireless sensor networks,” *Wireless Communications, IEEE*, vol. 15, no. 4, pp. 60–66, Aug 2008.

[6] J. Dong, K. E. Ackermann, B. Bavar, and C. Nita-Rotaru, “Secure and robust virtual coordinate system in wireless sensor networks,” *ACM Trans. Sen. Netw.*, vol. 6, no. 4, pp. 29:1–29:34, Jul. 2010. [Online]. Available: http://doi.acm.org/10.1145/1777406.1777408

[7] A. Jøsang and R. Ismail, “The beta reputation system,” in *In Proceedings of the 15th Bled Electronic Commerce Conference*, 2002.

[8] D. Dhanapala and A. Jayasumana, “Anchor selection and topology preserving maps in WSNs – 2014; a directional virtual coordinate based approach,” in *Local Computer Networks (LCN), 2011 IEEE 36th Conference on*, Oct 2011, pp. 571–579.

[9] “CSU sensor-net benchmarks,,” Available: http://www.cnrl.colostate.edu/Projects/VCS/Sensor-Net.html.

[10] D. Bose, “Security of virtual coordinate based wireless sensor networks,” Ph.D. dissertation, Colorado State University, Fort Collins, July 2015.