# Proactive Reputation-Based Defense for MANETs Using Radial Basis Function Neural Networks

Eyosias Y. Imana, *Student Member, IEEE*, Fredric M. Ham, *Fellow, IEEE*, William Allen, Richard Ford

***Abstract*— We have developed a proactive reputation-based defense system for Mobile *ad hoc* Networks (MANETs). In our work we assume the existence of nodal attributes which have the potential to affect the reputation score of a node at anytime. A radial basis function neural network (RBF-NN) is trained to learn the underlying mapping between the states of the various nodal attributes and the reputation score for the node at future times. Thus, the RBF-NN can be used to predict the reputation score of a particular node ahead of time, given only the current state of the node's attributes. Such a predictive system can result in lowering the reputation score of a node that is *about* to start malicious activity in *advance* of the actual attack. The RBF-NN predictors developed in this research to implement the proactive defense system resulted in an overall performance of 98.7% correct prediction with a 10-step predictor, and for comparison purposes, 98.1% with a 15-step predictor.**

*Keywords- MANET, proactive defense, RBF-NN, reputation, trust, attribute*

## I. Introduction

A Mobile *ad hoc* Network (MANET) is a self-configuring network of mobile nodes which are communicating with each other through a wireless media. The member nodes form the network dynamically without the use of any centralized infrastructure. To relay packets between each other, nodes also function as routers in MANETs. This means packets need to hop through one or more intermediate nodes to reach to their destination. These characteristics can result in vulnerabilities in a MANET. For example, there is no guarantee that every node though which a packet is routed is *benign.* Typically, compromised nodes eavesdrop, misroute or alter contents of the packets that are relayed through them [1]. Hence, there should be a controlling scheme which determines the *trustworthiness* of each node in the network. This controlling scheme can be used as a defense system to protect the network from an attack originating from compromised member nodes.

A defense system for a MANET should be capable of detecting compromised nodes from the network in real time. Then the defense system ensures that all the other nodes limit their interaction with compromised malicious nodes so that such nodes systematically get *quarantined* from the rest of the network.

A trust/reputation based defense system [2-7] is one of the most recognized types of defense systems used in MANETs. Such a defense system operates by assigning reputation scores for each node based on the type of nodal activities that are perceived by the rest of the network. For example, if a node is observed dropping packets rather than routing them to appropriate neighbors, it is assigned a lower reputation score. Hence, at a later time, other nodes will be reluctant to route their packets through this node.

However, defense systems proposed in [2-7] assign the reputation score of a node *reactively*. Hence, a mobile node which is performing malicious activities is assigned a bad reputation score some time after the actual activity begins. Therefore, the malicious node continues attacking the network until the defense system detects the maliciousness and countermeasures are taken. However, it stands to reason that there is dependence between the reputation score of a node and its internal nodal state. Therefore, it should be possible to correlate internal states of a node with its reputation score. Internal states of nodes can be defined in terms of internal features or attributes which have the potential to affect the behavior of the node in the network [8]. Furthermore, these attributes might change with time, which implies that the overall state of the node is also potentially varying with time. Therefore, if the different states of each attribute and the reputation score are numerically represented, an algorithm can be developed to determine the mapping between any of the attribute values and the reputation score at a given time. Hence, the reputation score of the node can be determined by observing only the states of the attributes instead of observing the behavior or activities of the node. Moreover, advanced algorithms can be used to learn the pattern of the dynamics of each attribute with

Manuscript received January 26, 2010. This research is part of a multi-institutional effort, supported by the Army Research Laboratory via Cooperative Agreement No. W911NF-08-0023.

E. Y. Imana is with Virginia Polytechnic Institute, Blacksburg, VA USA (e-mail: eyosiasy@yahoo.com).

F. M. Ham is with the Electrical Engineering Department, Florida Tech, Melbourne, FL 32901 USA (Corresponding author, phone: 321-674-8138; fax: 321-674-8192; e-mail: fmh@fit.edu).

W. Allen and R. Ford are with the Computer Sciences Department, Florida Tech, Melbourne, FL 32901 USA (e-mail: wallen@fit.edu, rford@fit.edu).

978-1-4244-8126-2/10/$26.00 ©2010 IEEE

respect to time, and this in turn can be used to develop a reputation predictive capability at any MANET node. In other words, this would allow the determination of the reputation score of a node in advance of the start of some malicious activity, thus allowing

Countermeasures to be taken that could reduce the overall negative impact of this potentially afflicted node on the rest of the MANET.

Here we propose a proactive reputation-based defense system using a Radial Basis Function Neural Network (RBF-NN) to perform prediction of the nodal reputation score at future time steps. A simplified MANET is simulated to analyze the applicability of the proposed system. The simulated MANET contains nodes whose states change in accordance to the change of the state of the heuristic attributes.

This paper is organized as follows: Section II gives a brief overview of related work in this area. Section III describes the simulation approach taken for the network and the nodes. Section IV details the prediction algorithm, and Section V presents the prediction simulation results. Finally, Section VI concludes the paper by summarizing the contributions and further research.

## II. BACKGROUND

Marti et al. [2] proposed a defense system in which route selection is based on the reputation score of the nodes. The system is comprised of two components – the WatchDog and the PathRater. The WatchDog assigns reputation scores to each node based on the activity it displays as observed by its neighboring nodes. Then the PathRater selects the safest route a packet should follow based on the cumulative reputation score of the nodes along the possible routes.

Similarly, Buchegger and Le Boudec [3, 4] proposed the CONFIDANT protocol which detects and isolates misbehaving nodes in the network. The reputation score is determined by the observed or reported routing and forwarding behavior of nodes.

As previously mentioned, the defense techniques in [2-7] are unable to counter an attack *before* it starts. Based on this observation, the initial work by Ham et al. [8] suggested a proactive defense system which incorporates a RBF-NN to determine reputation scores of the node without observing the actual activity of the node. In [8] it is assumed that the reputation score of a node depends on the *internal state* of the node. Accordingly, the RBF-NN is first trained then used to map the internal state of the node to the reputation score at the same time step. Hence, the reputation score of the node is not assigned after the node has already started some malicious activity.

The defense system that is developed in this work is designed considering an attack generated by malicious codes propagating in a MANET. Malicious codes are commonly referred to as *worms*. Worms infect a node and eventually begin to transmit

| **Time** | **State of Node** | **Reactive Defense** | **Proactive Defense** | |
|---|---|---|---|---|
| | | | **One-Step Predictor** | **Multi-Step Predictor** |
| $n = n_o$ | | | | |
| $n = n_o + 1$ | | | | Detect Vulnerability |
| … | | | | Counter |
| … | | | | |
| … | Node attains a vulnerable state | | Detect Vulnerability | |
| | Node is compromised | | Counter | |
| | | | | |
| | | | | |
| | | | | |
| | Node Starts Malicious Activity | Detect Compromise | | |
| | | Counter | | |

Figure 1. Comparing various versions of reputation based defense systems for MANET.

their replicas and infect other victim nodes in the network. Moreover, worms are also able to initiate denial-of-service attacks from their hosts [9].

Similar to [8], this research assumes that a node is infected by a malicious code only if it is in a vulnerable state. It also assumes the existence of a trusted component residing at each node to report the values of the attributes to the unit in the network which hosts the defense system. An infected node gets compromised and begins malicious activities after the worm establishes itself in the system at the new host. Accordingly, reactive reputation-based defense systems detect the compromise after the node begins the malicious activities. Hence, reactive reputation-based defense alters the reputation score of a malicious node only *after* it starts the malicious activity. On the other hand, proactive reputation defense systems operate by predicting the reputation score of a node in advance of an attack, thus allowing for countermeasures to be taken in advance of a potential serious outbreak in the MANET. The proactive reputation-based defense system developed in this research uses a RBF-NN to predict the possible reputation score of a node at future time steps by determining if the node is going to attain a vulnerable state at the current time step, or in the near future.

The chart in Fig. 1 compares the operation of the reactive systems, one-step proactive systems, and multi-step proactive reputation-based defense systems.

## III. MODELING THE NETWORK AND THE NODES

The results reported in this paper are based simulations carried out at Florida Tech in the Information Processing Laboratory because data from actual field MANETs are not readily available. In the various simulations, a node is assumed to attain three different states. The first state is the state at which the node is vulnerable to an attack. If a node is attacked while it is on a vulnerable state, it will be *compromised.* A compromised node starts a malicious activity after a random number of time steps. A compromised node stops its malicious activity when it attains the *forgiveness* state. After attaining the forgiveness state, the node returns to the *benign* state.

Nodes in the simulations are heuristically modeled using ten attributes. The states of the various attributes define the overall state of the node which determines the reputation score of the node at a certain time. The ten attributes are features that are known to have an impact on the reputation score of a node. This type of modeling is very similar to the modeling that is used in [10]. Table I briefly describes the ten attributes that are used for the modeling in the simulations.

TABLE I. DESCRIPTIONS OF THE ATTRIBUTES THAT ARE MODELED IN THE SIMULATION

| Attribute | Description | Values | Example practical processes |
|---|---|---|---|
| Att. 1 | Increases with time. Initial value is 0. | 0-10 | Time |
| Att. 2 | Decreases with time. Initial value is 10. | 0-10 | Battery power |
| Att. 3 | Pseudo-random four level process | 0-4 | Type of encryption in use |
| Att. 4 | Pseudo-random binary process | 0,1 | Whether registry file X is accessed or not |
| Att. 5 | Pseudo-random binary process | 0,1 | Whether registry file Y is accessed or not |
| Att. 6 | Four state discrete Markov process | 1-4 | Type of patch in use for software A |
| Att. 7 | Four state discrete Markov process | 1-4 | Type of patch in use for software B |
| Att. 8 | Four state discrete Markov process | 1-4 | Type of patch in use for software C |
| Att. 9 | Four state discrete Markov process | 1-4 | Type of patch in use for software D |
| Att. 10 | Truncated-Poisson distrusted random process | Mean =3<br>Max. = 8 | Number of neighboring nodes at current the time step |

The vulnerable and forgiveness states at each node are defined in Table II. A node assumes a compromised state and eventually a malicious state right after it attains a vulnerable state and it is compromised while it is in the vulnerable state. A node will escape to a benign state from a malicious state only after it attains the forgiveness state.

The reputation value of a node varies between zero and one. In the simulations, the reputation value of the nodes is lowered by 0.01 per each time step if it is performing a malicious activity. The reputation score of a node starts increasing by 0.01 per time step after it stops performing malicious activities.

TABLE II. DEFINITIONS OF THE VULNERABLE AND FORGIVENESS STATE IN TERMS OF STATES OF ATTRIBUTES

| **Name** | **Vulnerable State** | **Forgiveness State** |
|---|---|---|
| Vul-1 | *Att*3 = 1, *Att*5 = 1, *Att*7 = 3 | *Att*9 = 4, *Att*8 = 4, *Att*5 = 0 |
| Vul-2 | *Att*2 < 2 | *Att*2 is reset |
| Vul-3 | *Att*3 = 1, *Att*6=4, *Att*7=3 | *Att*3=4, *Att*4=0, *Att*8 = 4 *Att*10<4 |

## IV. PREDICTOR

An RBF-NN is used to determine underlying mapping between the states of the various nodal attributes and the reputation score for the node at future times. This section describes how the RBF-NN is used to implement the predictor for proactive reputation-based defense systems.

Let the matrix $A_k \in \Re^{p\times q}$ (a matrix of integers), where p=1000 and q=10, contain the attribute row vectors generated for kth node for 1000 time steps. The vector $R_k \in \Re^{p\times 1}$ (p=1000) contains the assigned reputation values for each 1000 times steps.

$$A_k = \begin{bmatrix} a_1(0) & a_2(0) & \dots & a_{10}(0) \\ a_1(1) & \dots & \dots & a_{10}(1) \\ \dots & \dots & \dots & \dots \\ a_1(999) & \dots & \dots & a_{10}(999) \end{bmatrix}_{1000\times 10} \qquad (1)$$

$$R_k = \begin{bmatrix} r(0) \\ r(1) \\ \dots \\ r(999) \end{bmatrix}_{1000\times 1} \qquad (2)$$

A linear function $\hat{f}_n$ which approximates the function $f_n$, such that $r(n+P) = f_n(\underline{\varsigma}(n))$ needs to be estimated at each time step using a RBF-NN. The attribute vector $\underline{\varsigma}(n)$ is a $10\times 1$ vector comprised of the values of the 10 attributes at the $n^{\text{th}}$ time step as defined in (3). The value $r(n+P)$ is the reputation value at the $l^{th}$ time step, such that $l = n+P$, where $P$ is the lead time of the prediction. The actual reputation score at a time is represented by $r_{TR}(l)$ .

$$\underline{\varsigma}(n) = \begin{bmatrix} a_1(n) & a_2(n) & \dots & a_{10}(n) \end{bmatrix}_{1\times 10} \qquad (3)$$

The linear function $f_n$ is estimated by using the attribute data that is given in the recent past. The training data at $n^{\text{th}}$ time step, $A^n_{k,train}$, is defined in (4).

$$A^n_{k,train} = \begin{bmatrix} \underline{\varsigma}(n-N) \\ \underline{\varsigma}(n-N+1) \\ \dots \\ \underline{\varsigma}(n-1) \end{bmatrix}_{N\times 10} \qquad (4)$$

$$N = \min\{300, n\} \qquad (5)$$

The value $N$ is the number of attribute vectors (equation 3) in recent past that are used to train the RBF-NN at each time step. The value of $N$ is defined in (5). The higher the value of $N$, the slower will be the training algorithm. On the other hand, smaller values of $N$ reduce the effectiveness of the training and result in performance degradation. As it is mentioned previously, the training process at each time step estimates function $\hat{f}_n$ which approximates the function $f_n$, such that $r(n+P) = f_n(\underline{\varsigma}(n))$.

The reputation score after $P$ time steps, $\hat{r}(n+P) = \hat{f}_n(\underline{\varsigma}(n))$, is determined using $A^{n}_{k,train}$ from the $n^{th}$ time step. Finally, the reputation score $\hat{r}_{TR}$ is computed by thresholding the estimated reputation value $\hat{r}$ by $TR = 0.5$.

## V. RESULTS

The predictive performance of the RBF-NN is determined by comparing the thresholded reputation score estimate by the proactive defense system, $\hat{r}_{TR}(l)$, with the actual (optimally assigned) reputation score, $r_{TR}(l)$, generated by the simulation at each $l^{th}$ time step. The neural network predictive performance at a node is computed as the percent of the ratio of the correct predictions to the total number of predictions.

The overall Reputation Prediction Performance (RPP) of the MANET is computed as the average of the individual performances of all the nodes. The simulation is run for 1000 time steps on 12 nodes. Figures 2 shows the results obtained at node 6 with a 10-step predictor. Table III lists the performance at each node for 10 and 15 step predictions. The proactive defense system predictor produced an RPP of 98.69% with a 10-step predictor and RPP of 98.08% for a 15-step predictor.

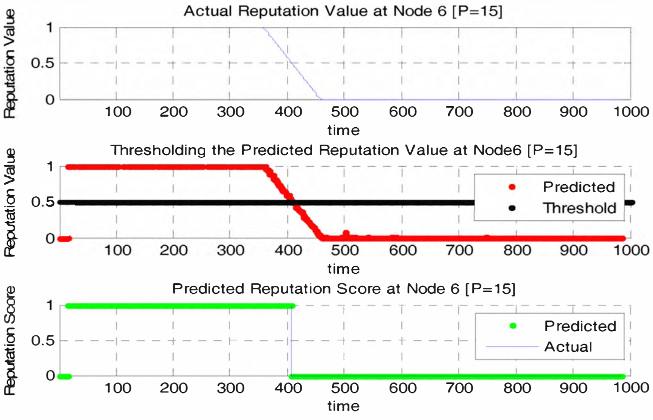

Figure 2. Prediction performance at node 6.

TABLE III. PREDICTION PERFORMANCE AT EACH NODE

| **Node** | **10 Step** | **15 Step** |
|---|---|---|
| Node 1 | 98.59% | 98.17% |
| Node 2 | 98.49% | 98.27% |
| Node 3 | 98.59% | 98.87% |
| Node 4 | 98.69% | 97.56% |
| Node 5 | 98.79% | 98.27% |
| Node 6 | 98.79% | 98.17% |
| Node 7 | 98.49% | 98.27% |
| Node 8 | 98.79% | 98.27% |
| Node 9 | 98.69% | 97.97% |
| Node 10 | 98.79% | 98.17% |
| Node 11 | 98.79% | 98.17% |
| Node 12 | 98.79% | 98.77% |
| **Average** | **98.69%** | **98.08%** |

## VI. CONCLUSIONS

This paper presents a proactive reputation-based defense system with a multi-step capability. Multi-step proactive defense allows the initiation of countermeasures on malicious nodes in advance of an attack. The proactive defense system predictor produced an RPP of 98.7% with a 10-step predictor and, for comparison purposed, a RPP of 98.1% was achieved for a 15-step predictor.

We are planning future research that includes conducting more in-depth investigations into the various systems attached to the nodes in a MANET in order to identify other attributes which could have a significant impact on the reputation score of the nodes. It is also planned to enhance the performance of the predictor by adding adaptive features to the algorithm.

## REFERENCES

[1] B. Wu, J. Chen, J. Wu, M. Cardei, "A survey of attack and countermeasures in mobile ad hoc networks," Book Chapter in Wireless Network Security, Y. Xiao, X. Shen, D.Z. Du, Springer Science+Business Media LLC, NY, USA, 2007.

[2] S. Marti, T. Giuli, K. Lai, M. Baker, "Mitigating routing Misbehavior in Mobile Ad Hoc Networks." In the proceedings of the *Sixth International Conference on Mobile Computing and Networking*, pp. 255-265, August 2000.

[3] S. Buchegger, J.Y. Le Boudec, "Nodes Bearing Grudges: Towards Routing Security, Fairness, and Robustness in Mobile ad hoc Networks." In the proceedings of the *10th Euromicro Workshop and Parallel, Distributed and Network-Based Processing*, pp. 403-410, 2002.

[4] S. Buchegger, J.Y. Le Boudec, "Performance Analysis of the CONFIDANT Protocol: Cooperation of Nodes–Fairness in Dynamic ad-hoc Networks." In the proceedings of the *IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing*, pp. 226-236 , June 2002.

[5] L. Abusalah, A. Khokhar, G. BenBrahim, W. ElHaij, “TARP: Trust-Aware Routing Protocol.” In the proceeding of the *2006 International Conference on Communications and Mobile Computing (IWCMC)*, pp. 135 – 140, 2006.

[6] W. Gong, Z. You, D. Chen, X. Zhao, M. Gu, K-Y. Lau, “Trust based malicious nodes detection in a MANET.” In the proceedings of International Conference on E-business and Information System Security, pp. 1-4, 2009.

[7] S. Kpodjedu, S. Pierre, M. Poursandi, “Reputation based trust management using TCG in Mobile Ad-Hoc Networks (RTA).” In the prodeedings of 33rd IEEE Conferenence on Local Computer Networks, pp. 518 -519, 2008.

[8] F. M. Ham, E. Y. Imana, W. Allen, R. Ford, A. Ondi, “Reputation Prediction in Mobile ad hoc Networks Using RBF Neural Networks.” In the proceedings of the *11th Annual International Conference on Engineering Applications of Neural Networks (EANN)*, London, August 27-29, 2009, pp. 485-494.

[9] N. Weave, V. Paxson, S. Staniford, R. Cunningham. “A taxonomy of computer networks,” In the proceedings of the *ACM workshop on rapid malacode*, Washington DC, pp. 11- 18, 2009.

[10] E. Y. Imana, “A Proactive Defense System for Mobile ad hoc Networks (MANETs)”, Masters Thesis, Florida Institute of Technology, December 2009.