A Trusted Framework for Secure Routing in Wireless Ad Hoc Networks

Waleed S. Alnumay
Computer Science Department
King Saud University
Riyadh, Saudi Arabia
wnumay@ksu.edu.sa

Pushpita Chatterjee
SRM Research Institute
Bangalore, India
pushpita.c@res.srmuniv.ac.in

Uttam Ghosh
Dept. of E & ECE
Indian Institute of Technology Kharagpur
Kharagpur, India
uttamg@iitkgp.ac.in

***Abstract*—This paper proposes a novel quantitative trust model that supports both first-hand (direct) and second-hand (recommendation) trust opinion to calculate the final trust of each node in the network. In order to compute direct trust of a node, the proposed trust model utilizes the theory of ARMA/GARCH to predict the trust parameters and a probabilistic model to combine those parameters. The proposed trust model collects recommendation trusts from common neighbors of the node under review and combines these trusts to get the resultant trust using a weighted combination model. Based on proposed trust model, a routing protocol has been driven to provide trustworthy routes. Simulation results show that the proposed protocol gives significantly higher packet delivery fraction as compared to CBRP even in presence of malicious nodes in the network. In summary, our proposed model is lightweight in terms of computation and powerful in terms of flexibility and accuracy in managing trust in WANET.**

***Keywords*—WANET, Trust, ARMA, GARCH, Security**

I. Introduction

A Wireless Ad Hoc Network (WANET) is a decentralized distributed collection of wireless mobile nodes. It is an infrastructure-less dynamic network due to node mobility. Such networks support multi-hop routing and they have wide-ranging applications ranging from military scenarios, infrastructure monitoring, and distributed data processing. There are significant differences in such networks from traditional networks. One noted factor is the limited processing capabilities and available power at the individual terminals. From the operative point of view, these networks primarily depend on broadcast nature of the communication medium. Further, lack of reliability of the wireless medium poses challenge to such networks. In recent years, significant research is carried out to manage these vulnerabilities in order to develop efficient protocols for a WANET.

Trust can play an important role to ensure and improve security of these networks by a-priori or runtime evaluation of trustworthiness of its peers before making any routing decision. Due to the quasi-static and distributed nature of nodes, WANETs are susceptible to various types of attacks [1]. Node cooperation significantly increases the performance of the network. Here "cooperation" means that the willingness of a node to sacrifice its resources (e.g., energy, bandwidth) for the benefit of other nodes in the network. Most of the applications of WANETs assume that all nodes are cooperative in nature. However, it can be seen that nodes may behave as legitimate participants in the initial stage in a collaborative group, and therefore pass the traditional cryptographic verifications. In the later stage, they could turn out to be selfish players and report false measurements either with malicious intentions or due to faulty components.

Cryptographic mechanisms cannot help in order to detect/ prevent such kinds of behaviours as these behaviours are continuously changing. Such security threats can be handled effectively using trust management systems. Trust management cannot be seen as a complete replacement for cryptography, rather a supplement to it. As a second line of defence with cryptographic schemes, trust can play an important role to achieve such security goals. Trust management is needed when participating nodes, without any previous interactions, desire to establish a network with an acceptable level of trust relationship among them. Cryptography and trust management system can work together to provide holistic security solution in WANET. To achieve better accuracy, a trust decision framework should not assume that all nodes are cooperative in resource restricted environments. In recent years, several trust management schemes [2]–[10] and trust based routing protocols [11]–[18] have been designed and evaluated in ad hoc networking scenario.

Contribution: In this paper, we propose a novel quantitative trust management scheme that supports both first-hand (direct) and second-hand (recommendation) trust opinion to calculate the trust of a node under review. The trust parameters are predicted by utilizing the theory of ARMA/GARCH and a probabilistic model is used to combine those parameters in order to calculate the direct rating of trust of the node under review. Again by collecting recommendations from other common neighbours, trust evidences are combined to get the resultant trust using a weighted combination model. In this proposal, trust quantification model, and trust parameters are carefully selected such that these metrics have good impact towards proper network functionalities. Using ARMA/GARCH, next possible value is predicted for each trust parameter so

978-1-4673-7648-8/15/$31.00 ©2015 IEEE

that model can give better prediction for unseen data [19]. Using the of notion multilevel prediction, trust is quantified with a fairly good accuracy. Through extensive simulation, we evaluate the performance to show that our proposed trust model gives 0% false positive even when more than 20% packet drops in the network. Further, our trust based routing protocol outperforms CBRP [20] in terms of packet delivery fraction. In summary, our proposed model is lightweight in terms of computation and powerful in terms of flexibility and accuracy in managing trust in WANET.

Organization of the paper: The rest of the paper is organized as follows: Section II presents our proposed trust model for wireless ad hoc networks. In Section III, we present the simulation results of the proposed trust protocol along with an existing protocol. Finally, conclusions are presented in Section IV.

II. Proposed trust prediction model

In order to achieve reliable routing and data transmission in WANET, it is necessary to build a trustworthy framework. The mechanisms for clustering and clusterhead (CH) election are beyond the scope of the present paper. We consider the same clustering framework as described in [21] for clustering, CH election and initial setup of the network [22]. This paper deals with a trust model that calculates the trust of each node and provides a trustworthy route between source destination nodes.

A node X monitors traffic of each neighbor node Y and calculates the direct trust evidence ($Trust_{X,Y}(t)$) in a time period (τ_{Trust}).

Trust parameters are carefully chosen according to their contribution towards proper functioning of the network and find out a trustworthy route for secure end-to-end data delivery. These parameters are categorized as Good and Bad behavior in order to achieve reliable data delivery. Good parameters like number of packets properly forwarded and bad parameters like number of packets dropped.

After each time period of τ_{Trust}, node X calculates the value of each parameter and predicts direct trust observation using Beta distribution. Fig. 1 shows the system architecture of the proposed model. The trust generation model is presented in Fig. 2.

Trust Revocation Manager: This module of CH decides when to initiate trust calculation. If trust calculation is performed periodically then it requires a lot of processing time and power. Further, one-time trust calculation is not a suitable solution due to the quasi-static nature (node mobility) and uncertain behavior of mobile nodes (e.g., selfishness in order to save their power) which incurs different trust evidences (trust parameters). Thus there should be a trade-off between the trust revocation and trust initialization. This manager assigns an aging factor to each trust value which feeds the trust value. This factor is application specific and it can be set depending upon the requirement.

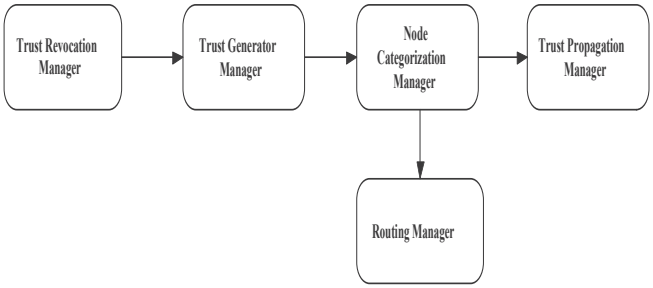

Figure 1. System Architecture

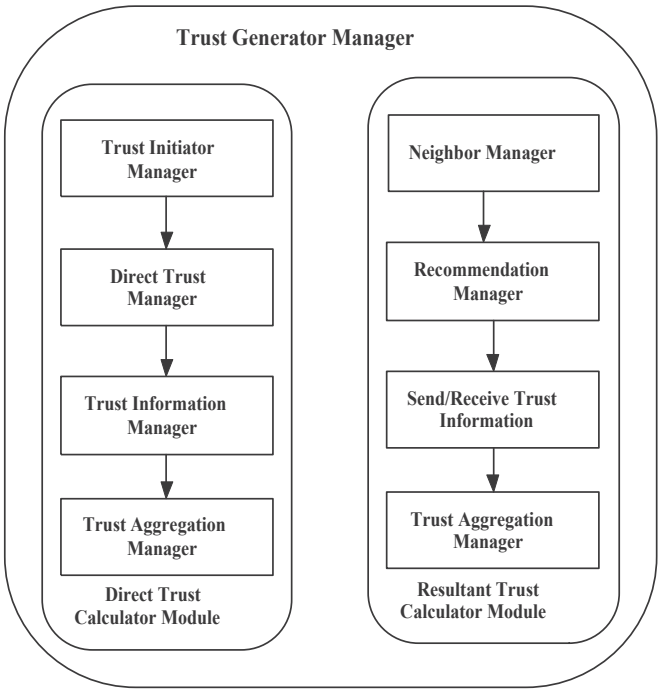

Figure 2. Trust Generation Model

Trust Generator Manager: This module resides in each member and CH of a cluster. It is responsible for calculating trust of each member of a cluster. The overall trust generation procedure is described below.

Node Category Manager: Once CH calculates the resultant trust of members, this module categorizes the cluster member according to its resultant trust value:

- Good, if trust value $\geq$ max-threshold
- Bad, if trust value $\leq$ min-threshold
- Uncertain, if min-threshold $<$ trust value $<$ max-threshold.

Trust Propagation Manager: After calculating the resultant trust of each member node, this module of CH propagates those trust values to the member nodes. In order to provide more accuracy and reduce redundancy in the present model,

only CH is entitled to propagate the final trust values of member nodes.

Routing Manager: It resides in each member and CH of a cluster. The responsibility of routing manager is to find out the best possible route from source to destination. Routing manager consists of the following three modules:

- Neighbor discovery is responsible for maintaining list of neighbors along with their trust status.
- Route discovery module is responsible for finding route between source and destination. For reliable routing, only good and uncertain nodes can participate in routing.
- Route maintenance module is responsible for maintaining the route and re-initiating the route discovery whenever route error occurs due to link failure.

Trust Generator Manager Direct Trust Calculator Module:

Trust Initiator Manager: At the time bootstrapping, this module of CH and cluster members initiate the trust calculation procedure. Once the trust value is aged, trust revocation manager initiates the trust calculation by calling trust initiator manager. Further, trust initiator manager activates the trust information manager module.

Trust Information Manager: This module resides in CH and cluster members. The major functionalities of this module are to collect the good and bad trust evidences or metrics. Good evidence like the number of packets forwarded by a node and bad evidence like number of packets dropped by a particular node or similar adverse deeds.

Trust Aggregation Manager: This module works in each member and CH of a cluster. Trust information manager at each node collects and stores collective data for all good and bad events. In order to calculate direct trust, a reputation system based on the Beta probability density function has been used. Beta function is useful to represent probability distributions of binary events (either good or bad). This provides a sound mathematical basis for combining feedback and expressing reputation ratings. For example, if node X has collective information of positive (good) and negative (bad) behaviors about a node Y which are α, and β respectively, then the posterior probabilities of trust value can be predicted using Beta distribution function is presented in Eqn. 1. The Beta distribution can be expressed using the gamma function as

$$f(p|\alpha,\beta) = \frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)+\Gamma(\beta)} p^{(\alpha-1)}(1-p)^{(\beta-1)} \tag{1}$$

Where $0 \leq p \leq 1$, $\alpha, \beta > 0$, with the restriction that the probability variable $p \neq 0$ if $\alpha < 1$, and $p \neq 1$ if $\beta < 1$.

It is an uncertain probability and the expected probability of trust value is $E(p)$. Therefore it can be said that the relative frequency of outcome is most likely to be $E(p)$. The direct trust of a node under review can be calculated using Eqn 2.

$$E(p) = \alpha/(\alpha+\beta) \tag{2}$$

Once calculated each node stores its own trust opinion about its neighbors.

Resultant Trust Calculator Module:

Neighbor Manager: This module resides in each member and CH of a cluster. CH sends HELLO beacon periodically to keep the track and maintain a list of node IDs of members (or neighbors) in the cluster. Each member also maintains a list of node IDs (or neighbors) by exchanging periodic HELLO messages.

Send/Receive Trust Information: This module resides in CH. At the time of resultant trust calculation of a node under review, it collects the list of common neighbors of the target node from Neighbor manager. Then it multicasts a $< send\_trust >$ request message with target node_ID to them. On receiving $< send\_trust >$ request message, each member node verifies its list of neighbors. If the member node finds out that the target node is in its neighbor list, it sends the recommended trust (i.e, its trust opinion about the target node) to CH. On receiving the individual trust opinions from different member nodes, this module of CH checks the redundancy and stores the recommended trust information.

Trust Aggregation Manager: This module resides in CH only. Once receives all the recommendation trust evidences by CH from the member nodes, this module executes ARMA(1,1)/GARCH(1,1) to calculate the resultant or final trust of a node under review. The resultant trust calculation procedure using ARMA(1,1) is described in Eqn.3.

$$X_t = \varepsilon_t + \Sigma_{i=1}^{p} \varphi_i X_{t-i} + \Sigma_{i=1}^{p} \theta_i X_{t-i} \tag{3}$$

To estimate ε_t which is s independent (where s is set of independent trust evidences collected from common neighbors and self evidence also) following normal distribution with zero mean and constant variance σ_ε^2. So, the likelihood function for the ARMA (1,1) model [19] is

$$L(\varphi_1\theta_1, \sigma_\varepsilon^2) = \prod_{t=2}^{T} \frac{1}{\sqrt{2\Pi}\sigma_\varepsilon} \times \exp\{-\frac{(y_t - c - \varphi_1 y_{t-1} - \theta_1 \varepsilon_{t-1}^*)^2}{2\sigma_\varepsilon^2}\} \tag{4}$$

Therefore the log likelihood function is

$$l(\varphi_1\theta_1, \sigma_\varepsilon^2) = -(T-1)\log\sigma_\varepsilon - \frac{1}{2\sigma_\varepsilon^2} \times \sum_{t=2}^{T} (y_t - c - \varphi_1 y_{t-1} - \theta_1 \varepsilon_{t-1}^*)^2 \tag{5}$$

where $\varepsilon_t^* = y_{t-1} - c - \varphi_1 y_{t-2} - \theta_1 \varepsilon_{t-2}^*$ for $t = 3, ..., T$ are

obtained recursively.

The GARCH (1, 1) model is expressed as

$$\sigma_t^2 = k + G_1\sigma_{t-1}^2 + A\varepsilon_{t-1}^2 \tag{6}$$

where $\sigma_t^2\varepsilon_t$ is taken from ARMA(1,1) model and it assumes that it has conditional variance ε_t^2. In case of Gaussian ε_t, the likelihood function is

$$L(k, G^1, A_1) = \prod_{t=2}^{T} \frac{1}{\sqrt{2\Pi}\varepsilon_t} \exp\{-\frac{\varepsilon_t^2}{2\sigma_{\sigma_t^2}^2}\} \tag{7}$$

The log likelihood function, neglecting the constant term can be written as

$$l(k, G^1, A_1) = \frac{1}{2}\sum_{t=2}^{T}\{\log\sigma_t^2 + \frac{\varepsilon_t^2}{\sigma_t^2}\} \tag{8}$$

where $\sigma_t^2 = k + G_1\sigma_{t-1}^2 + A_1\varepsilon_{t-1}^2$ are obtained recursively. Therefore after collecting trust evidences from common neighbors the ARMA/GARCH model is used to predict the multiple-step ahead value of the trust series. In our work, trust is predicted with higher accuracy and multiple step ahead prediction is used to ensure the trustworthiness of a node. Using this model a more reliable end-to-end route can be set with trusted neighbors for even large data stream.

III. Simulation

To show the efficacy of the propose trust based routing protocol we have compared the performance of our scheme with CBRP [20]. We have implemented all these routing protocols on top of AODV using NS-2 (version-2.34) simulator [23].

A. Simulation Parameters

In the simulation, IEEE 802.11 standard has been used as the MAC layer protocol. The transmission range of each node is set to 250m and the nodes follow random way-point mobility model. The speed of the mobile nodes is varied from 0m/s to 5m/s and on reaching the destination the pause time is set to 5s. Two ray ground is used as the propagation model. UDP has been used as the transport layer protocol with constant bit rate (CBR) traffic generator of packet size 512bytes. Simulation is done for 500s with 21-nodes cluster over a network area of 450m*450m. The summary of simulation parameters are shown in Table I.

False positive is chosen as the performance metric to evaluate the proposed trust model. False positive refers to the ratio of number of good nodes falsely detected as malicious and total number of nodes in the network. Here we vary the rate of packet collision to plot the false positive of the proposed trust model. It may be noted that this packet collision includes the packet drops by the malicious nodes. Further, we consider two levels of security, namely *High* and *Low*. In *High* level of security, max_threshold and min_threshold

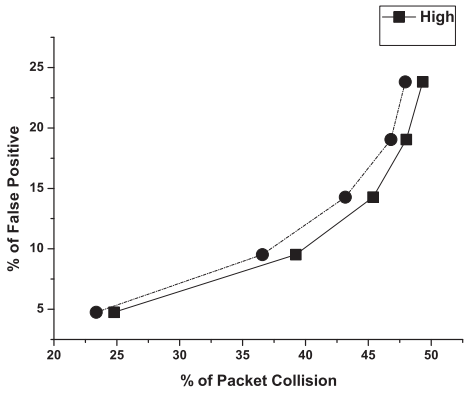

Figure 3. False Positive Vrs. Packet Collision

are set to 0.7 and 0.4 respectively. Whereas in *Low* level of security, max_threshold and min_threshold are set to 0.6 and 0.3 respectively. Initial trust value of each node is set to 0.5 for both levels. Figure 3 presents the percentage of packet collision versus percentage of false positive of the proposed trust model for both levels of security. It can be seen that nearly 5% nodes are falsely detected as malicious when 24.78% and 23.36% packet collisions occur for *Low* level and *High* level respectively. Further, the proposed trust model falsely detects nearly 24% nodes as malicious when 49.32% and 47.93% packet collisions taken place for *Low* level and *High* level respectively. Therefore, the proposed trust model performs well even when the rate of packet collision is high in the network. Also, it depends on max_threshold and min_threshold parameters, and the values of those parameters can be set according to the application scenario.

In order to compare the proposed trust based routing protocol with CBRP [20], packet delivery fraction (PDF) and packet drop rate (PDR) have been chosen as the performance metrics. Figure 4 and Figure 5 show the effect of malicious node on PDF and PDR respectively for both protocols under consideration. It can be seen that both protocols give more than

TABLE I
Simulation Parameters and Environment

Simulation Parameter	Assigned Value
Application Agent	CBR
Packet Size	512 bytes
Transport Agent	UDP
Routing Protocol	AODV
Addressing Scheme	IDDIP
Mobility	0 - 5m/s
Pause Time	5s
Simulation Time	500s
Mobility Model	Random Way-Point
Network area	450 X 450
No. of nodes	21
No. of malicious nodes	5

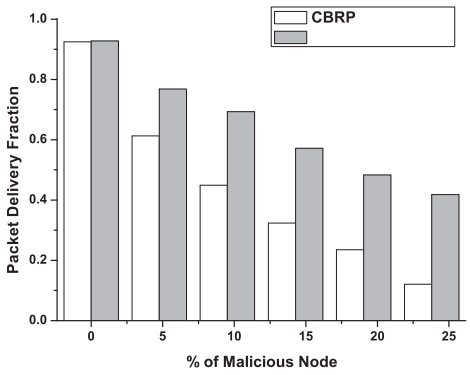

Figure 4. Packet Delivery Fraction Vrs. % of Malicious Node

0.9 as packet delivery fraction in absence of malicious node. However, PDR increases and subsequently PDF decreases with the increased number of malicious node for all protocols. CBRP gives 0.61 and 0.12 as PDF when nearly 5% and 24% malicious nodes present in the network respectively. Whereas the proposed protocol gives 0.77 and 0.42 as PDF for the same percentages of malicious nodes. From Figure 5, we can see that PDR increases from 0.41 to 0.89 when the number of malicious node increases from about 5% to 24% in case of CBRP. For the same percentages of malicious node, PDR increases from 0.17 to 0.45 in case of our proposed protocol. This is due to the fact that CBRP does not consider the security aspects in route discovery procedure and hence the malicious nodes may reside on the route and drop packets. The proposed protocol considers the security aspects and computes the trustworthy route by eliminating the malicious nodes.

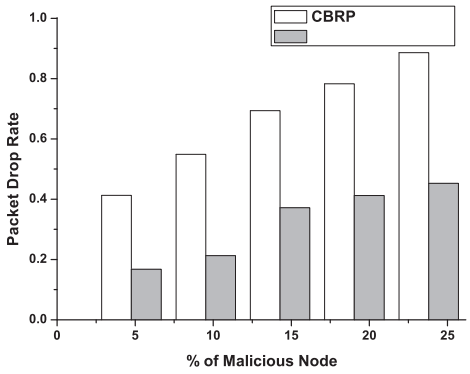

Figure 5. Packet Drop Rate Vrs. % of Malicious Node

IV. Conclusion

In this paper, we have proposed a novel quantitative trust model for wireless ad hoc networks that collaboratively computes the resultant trust of a node using direct trust and recommendation trust opinions from other nodes. The proposed trust model utilizes the theory of ARMA/GARCH and a probabilistic model to calculate direct trust of a node under review. In order to compute resultant trust of the node under review, the proposed trust model also collects recommendation trusts from common neighbors and combines them using a weighted combination model. A routing protocol has been derived from the proposed trust model that computes the trustworthy routes. Simulation results are given to show that the proposed trust model performs well in terms of false positive even when the network is highly congested. Further, the proposed trust based routing protocol outperforms CBRP in terms of packet delivery fraction and packet drop rate.

References

[1] S. Jain, T. Ta, and J. Baras, "Wormhole detection using channel characteristics," in *ICC, 2012 Proceedings IEEE*, pp. 6699– 6704, 2012.

[2] J. H. Cho, A. Swami, and I. R. Chen, "Modeling and analysis of trust management for cognitive mission-driven group communication systems in mobile ad hoc networks," in *Proceedings International Conference on Computational Science and Engineering*, pp. 641–650, Lecture Notes in Computer Science, August 29-31 2009.

[3] A. Boukerche and Y. Ren, "A security management scheme using a novel computational reputation model for wireless and mobile ad hoc networks," in *Proceedings of Intl Workshop on Modeling Analysis and Simulation of Wireless and Mobile Systems*, pp. 88–95, 23-24 March 2008.

[4] Z. Yan, P. Zhang, and T. Virtanen, "Trust evaluation based security solution in ad hoc networks," in *Proceedings of Seventh Nordic Workshop on Secure IT Systems*, 2003.

[5] B. J. Chang and S. L. Kuo, "Markov chain trust model for trust value analysis and key management in distributed multicast manets," *IEEE Trans. Veh. Technology*, vol. 58, pp. 1846–1863, May 2009.

[6] R. Li, J. Li, P. Liu, and H. H. Chen, "On demand public key management for mobile ad hoc networks," *Wileys Wireless Communications and Mobile Computing*, vol. 6, 2006.

[7] M. Virendra, M. Jadliwala, M. Chandrasekaran, and S. Upadhyaya, "Quantifying trust in mobile ad-hoc networks," in *Proceedings of IEEE International Conference on Integration of Knowledge Intensive Multi-Agent Systems KIMAS'05*, pp. 65–71, 2005.

[8] A. A. Pirzada, C. McDonald, and A. Datta, "Performance comparison of trust-based reactive routing protocols," *IEEE Transaction on Mobile Computing*, vol. 5, 2006.

[9] P. Chatterjee, U. Ghosh, I. Sengupta, and S. Ghosh, "A trust enhanced secure clustering framework for wireless ad hoc networks," *Wireless Networks*, vol. 20, no. 7, pp. 1669–1684, 2014.

[10] K. Govindan and P. Mohapatra, "Trust computations and trust dynamics in mobile adhoc networks: A survey," *Communications Surveys Tutorials, IEEE*, vol. 14, pp. 279–298, Second 2012.

[11] R. K. Nekkanti and C. Lee, "Trust-based adaptive on demand ad hoc routing protocol," in *Proceedings of 42th Annual ACM Southeast Regional Conf.*, pp. 88–93, 2004.

[12] A. A. Pirzada and C. McDonald, "Establishing trust in pure ad-hoc networks," in *Proceedings of 27th conference on Australasian computer science CRPIT'04 and Australian Computer Society and Inc*, 2004.

[13] T. Ghosh, N. Pissinou, and K. Makki, "Collaborative trust-based routing in multi-hop ad hoc networks," in *Proceedings of Proc. 3rd Intl IFIP-TC06 Networking Conf*, pp. 1446–1451, Lecture Notes in Computer Science, May 9-14 2004.

[14] T. Ghosh, N. Pissinou, and K. Makki, "Towards designing a trust routing solution in mobile ad hoc networks," *Mobile Networks and Applications*, vol. 10, pp. 985–995, 2005.

[15] L. Ruidong, L. Jie, L. Peng, and H.-H. Chen, "An objective trust management framework for mobile ad hoc networks," in *Proceedings of IEEE 65th Vehicular Technology Conference, 2007*, pp. 56–60, April 2007.

[16] L. Abusalah, A. Khokhar, and M. Guizani, "A survey of secure mobile ad hoc routing protocols," *IEEE Communication on Surveys and Tutorials*, vol. 19, 2008.

[17] X. Wang, L. Liu, and J. Su, "Rlm: A general model for trust representation and aggregation," *IEEE Transactions on Services Computing*, vol. 99, 2010.

[18] S. Liu, Y. Yang, and W. Wang, "Research of {AODV} routing protocol for ad hoc networks1," {*AASRI*} *Procedia*, vol. 5, no. 0, pp. 21 – 31, 2013. 2013 {AASRI} Conference on Parallel and Distributed Computing and Systems.

[19] H. T. Pham and B. S. Yang, "Estimation and forecasting of machine health condition using arma/garch model," *Mechanical Systems and Signal Processing*, pp. 546–558, 2010.

[20] C.-C. Chiang, H.-K. Wu, W. Liu, and M. Gerla, "Routing in clustered multihop, mobile wireless networks with fading channel," in *IEEE Singapore International Conference on Networks, SICON'97, April 16-17, 1997, Singapore*, pp. 197–211, April 1997.

[21] P. Chatterjee, I. Sengupta, and S. Ghosh, "A distributed trust model for securing mobile ad hoc networks," *Embedded and Ubiquitous Computing, IEEE/IFIP International Conference on*, vol. 0, pp. 818–825, 2010.

[22] U. Ghosh and R. Datta, "A secure dynamic ip configuration scheme for mobile ad hoc networks," *Ad Hoc Networks*, vol. 9, no. 7, pp. 1327–1342, 2011.

[23] K. Fall and K. Varadhan, "ns manual." isi.edu/nsnam/ns/doc.