Defence Science Journal, Vol. 62, No. 3, May 2012, pp. 167-173, DOI: 10.14429/dsj.62.1431

Implementation of a Regression-based Trust Model in a Wireless Ad hoc Testbed

Revathi Venkataraman*, M. Pushpalatha, and T. Rama Rao

SRM University, Kattankulathur-603 203, India
**E-mail: revathi.n@ktr.srmuniv.ac.in*

ABSTRACT

Wireless ad hoc networks are resource constraint and vulnerable to various security attacks. Trust based security modelling go hand in hand with cryptographic services to offer good security services. We have implemented a vector auto regression (VAR) based trust model over ad hoc on demand distance vector protocol and optimised link state routing protocol. The novelty in this model lies in capturing individual functional behaviours of a neighbour in an ad hoc network and modeling them as regression parameters. The experimental results show the feasibility of implementing trust models over real ad hoc network deployments. The simulations results show that the proposed VAR trust model offers better performance compared to the existing trust models.

Keywords: Ad hoc on demand distance vector, optimised link state routing, vector auto regression trust, econometric trust model

1. INTRODUCTION

Mobile networks have significant applications in the defence arena. With the move towards the network centric warfare, the information technology is expected to provide force multiplication effect to the military commanders in the future battlefield scenario. It also provides services on demand to the various echelons of the defence forces. Though an umpteen number of ad hoc networking protocols were developed, analyzed, simulated, and benchmarked over the last decade, lack of realism in a real application scenario is one of the reasons for the insufficient deployment of mobile ad hoc network (MANET) in military communications.

In addition, these networks are confronted by many types of attacks like passive eavesdropping, active modification of messages, and disruption of service, replay attacks and impersonation attacks[1,2]. The resource constraint environment poses a great challenge to the implementation of cryptographic security schemes in an ad hoc scenario due to their computational complexity. Additionally, a legitimate ad hoc node may behave maliciously due to compromise and remain undetected in the network. At a later time, these nodes may launch denial-of-service attacks. The cryptographic schemes fail to detect these nodes whereas the trust based security schemes easily identify these behavioural anomalies by monitoring the neighbours periodically.

In wireless applications, the satisfaction of the clients is achieved by successful message delivery with minimal delay. The average satisfaction level of the clients in a wireless ad hoc network is computed by aggregating the individual satisfaction levels of each of these clients. Some of the clients are victimized by malicious neighbours, thereby depriving them of their network resources. These behaviours are not accounted in the outcome. The trust and reputation schemes play a major role in identifying such functional misbehaviours of participating entities in the network.

Trust is defined as the assured reliance on the ability and truthfulness of another entity over a specific behaviour or action. It is subjective in nature, depending on the node's independent evaluations about other neighbouring nodes. In an ad hoc network, this process is done by continuous monitoring mechanisms. This dynamic real time view of trust will result in a more flexible model that resembles the social trust relations in humans. The positive outcomes of interactions will increase the trust, while negative outcomes lower the trust of a neighbouring entity.

The proposed vector auto regression (VAR) based trust model is an econometric statistical model where an ad hoc node adopts a node centric approach[3], but without any recommendation trust and depends on its own observations for evaluating a neighbour. The novelty in proposed model is the presence of trust metrics by which the behaviour of the neighbouring entity is captured through promiscuous listening. A vector of trust metrics is used to evaluate every action of the neighbouring node and its inter-relationship wrt time. Another unique feature in proposed trust model is that neighbours indulging in more than one type of security attack can be easily detected by the regression co-relation coefficients.

The contributions of this paper are as follows:

- A vector auto regression-based trust model to predict the malicious activities of the neighbour in an ad hoc network is proposed.
- The proposed trust model is implemented over ad hoc on-demand distance vector protocol and optimised link state routing protocol in a wireless ad hoc testbed. The feasibility of incorporating a trust model over ad hoc routing protocols is also practically demonstrated.

Received 16 January 2012, revised 3 April 2012, online published 3 May 2012

- The performance of the VAR trust model is compared with existing trust models and it was shown that the proposed model has capabilities to identify malicious nodes launching multiple attacks.

2. RELATED WORKS

The MANET research is focused on development of multi-hop wireless ad hoc network protocols and plenty of simulation analysis is performed on security issues as well[3-9]. For large-scale deployment of ad hoc networks, their performance with the security add-ons has to be tested in real time environment[10,11] and this may unfold many implementation issues.

The trust mechanism in each deployed mobile node should be capable of identifying a broad range of security attacks. In practical defence applications, an attacker node may launch multiple security attacks against its neighbour and the existing statistical trust models[3-5] have limited capabilities and does not provide a comprehensive framework to capture all behavioural and functional aspects of these neighbouring entities. The moving average model is predominantly used in literature[3-5,12] to compute the trust of a neighbouring node. These models evaluate trust as a single variable which does not truly reflect the multiple dimensions and behavioural aspects of neighbour's trust.

Security protocols employing cryptographic schemes are considered as hard security measures. Typical examples of such schemes, tailor-made for wireless sensor network (WSN) are SNEP[13], μTESLA[13] and LEAP[14]. SNEP offers data confidentiality, authentication and data freshness while μTESLA offers broadcast authentication. An agent based trust scheme[15] for WSN employs recommendation trust, similar to the trust based recommender system in tactical combat[16]. But, additional cryptographic message exchange overheads are incurred in the routing process.

All the above mentioned schemes fail to detect legitimate authorised nodes that misbehave due to compromise. The trust based security schemes offer soft security where authorized compromised nodes behaving maliciously over a period of time are detected easily by continuously monitoring their trustworthiness. Centralized trust schemes[17] aggregate the trust of individual nodes in a central server which evaluates the trust decisions of the participating nodes in the network. Such schemes are not suitable for MANETs since they lack centralized infrastructure. The proposed trust model is a node-centric approach which captures every functional aspect of the neighbouring nodes for ensuring complete security in MANETs.

3. VAR TRUST MODEL

The VAR is commonly used as a prediction tool in forecasting systems of interrelated time series. In the proposed work, the individual functional behaviour of a neighbouring entity is modelled as a single time series and it is termed as trust metric. A non-exhaustive list of trust metrics possible for proactive and reactive routing is shown in Table 1. These trust metrics depend on past values of themselves and the past values of other trust metrics for a neighbour node. Hence, the trust metrics are represented as endogenous variables. To detect multiple attacks launched by neighbours, it is necessary to take into account the interdependence between these time series. Hence, the VAR model is used which is a dynamic multi-equation system and a very useful tool in the analysis of interrelationships between the different time series[18].

Every node in the proposed model is entirely responsible for its trust decisions. The neighbour's trust is estimated using a VAR equation. Each vector entity indicates a trust metric. The neighbour's behaviour is captured in these individual vector trust metrics. Let n be the number of trust metrics to be evaluated. These metrics are represented as individual time series in the VAR model. In real network deployments, a malicious neighbour may launch multiple security attacks to create extensive damage to network resources. The proposed model aims to analyze the interrelationships between these trust metrics, thereby detecting multiple attacks launched by malicious neighbours at different instants of time.

The estimated trust vector of a neighbouring node y at time t is modelled as a VAR equation[18] and is given by Eqn (1).

Table 1. Generalised trust metrics for ad hoc routing

Parameter	Proactive routing	Reactive routing
T[1]	Number of TC messages received	Number of RREQs successfully forwarded
T[2]	Number of TC messages forwarded by neighbour	Number of RREQs received from the neighbouring node
T[3]	Number of occurrences showing the neighbour willingness to participate in data communication	Number of RREPs received from the neighbour
T[4]	Number of occurrences the neighbour is chosen as an MPR	Time taken to respond to a RREQ message.
T[5]	Number of DATA packets successfully forwarded by neighbour	
T[6]	Number of DATA packets received from the neighbour	
T[7]	Number of ACKs forwarded by the neighbour	
T[8]	Number of ACKs received from the neighbour	
T[9]	Number of DATA packets forwarded without content modification	

$$\hat{T}_{y(t)} = \sum_{i=1}^{p} R_i T_{y(t-i)} + \in_t \quad (1)$$

where $\hat{T}_{y(t)}$ is the estimated trust metrics vector of size n, R_i is a regression coefficient matrix of size $[n \times n]$, $\in_t$ denotes the error vector of size n and p is the time lag. The regression coefficients are determined by ordinary least square (OLS) estimates technique. These coefficients play a major role evaluating the neighbour's trustworthiness, especially, when more than one type of attack is launched by the neighbour. They also indicate the correlation between the different trust metrics of the neighbouring node and their past time-lagged values. The OLS equation for a trust metric, say T[1] for a time lag of 2 at time t is represented by Eqn (2).

$$T[1]_{y(t)} = \sum_{i=1}^{8} R'_{1i} T_{y(t-i)} + \sum_{i=1}^{8} R''_{1i} T_{y(t-i)} + \in_{1t} \quad (2)$$

Similarly, the VAR equation for the other trust metrics can be represented as shown in Eqn (2) where R' and R'' are the regression coefficient matrices in the first and second time lag respectively.

The estimated trust is normalised in the interval L_{max} and L_{min}. The normalised[19] trust for a neighbouring node y is computed from the vector equation as shown in Eqn (3).

$$T_y = \frac{(T_c - T_{min})(L_{max} - L_{min})}{T_{max} - T_{min}} + L_{min} \quad (3)$$

where T_c denotes the estimated trust vector, T_{max} and T_{min} are design parameters represented as vectors representing the maximum and minimum possible trust value. For example, T_{max} can be 0.9, taking into consideration the unreliable wireless links in an ad hoc environment and T_{min} can be –1 representing malicious behaviour. L_{max} is the upper bound on the trust range (+1) and L_{min} is the lower bound on the trust range (–1).

The confidence interval[19] of mean for the estimated trust is computed to determine the accuracy of the trust estimations. The standard confidence error for a single trust metric, about the mean is computed by Eqn (4).

$$\in = t \times \left(\frac{\sqrt{\frac{\sum_{i=1}^{j} (X_i - \bar{X})^2}{j-1}}}{\sqrt{j}} \right) \quad (4)$$

where t denotes the critical value obtained from the standard t-distribution for the 95 per cent confidence interval, j specifies the sample size and $\bar{X}$ denotes the mean value. It indicates the standard error of the mean multiplied by the critical value of t. The standard error is obtained by calculating the standard deviation of the data set over square root of the sample size.

The estimated trust is computed using the VAR model for each of the neighbouring nodes. A neighbour with a high trust value is chosen for data forwarding.

4. EXPERIMENTAL SETUP AND PERFORMANCE ANALYSIS

The proposed work is carried out in an ad hoc testbed with fifteen laptops in an indoor environment. The hardware comprises of Compaq 6510b laptops running Linux Mint version 10 and kernel 2.6.35.10 having Netfilter support and equipped with Intel PRO/Wireless 3945ABG. These devices serve as ad hoc nodes in indoor/outdoor environment. The AODV and OLSR versions, aodv-uu-0.9.6 and olsrd-0.9.6, from Uppasala University[20] serve as the default protocol versions. The customized trust modules are built over these default versions. The testbed for GUI based monitoring is developed using Python wxgtk-2.8. Front end interfaces are used to give instructions to the volunteers performing the test-runs in the testbed and initialize the node configuration parameters, time synchronization and the protocol specific parameters. At the end of the experiment, the logs from individual machines are uploaded to a central system and aggregation charts are prepared for the following performance metrics like throughput, delay, etc. Table 2 lists the experimental setup and configuration parameters for the testruns. The VAR time lag parameter (p) is chosen as 2 based on the Akaike's Information Criterion[19].

Table 2. Experimental setup parameters

Parameter	Value
Experimental area	600 × 600 m^2
Maximum node speed	20 m/s
Transmission range (indoor)	70 m (approx)
Number of nodes	15
Data packet size	50 bits
Duration of experiment	30 min
Channel data rate	11 Mbps
VAR time lag (p)	2
Number of trust metrics evaluated	8

4.1 Performance of AODV

The laptops participating in the ad hoc testbed are configured before the start of the experimentation through the python based GUI. Before the ad hoc network initiation, the participating nodes are synchronized in time. The AODV daemon is executed in each of these laptops. Raw data packets are transferred from a source to a destination using hping3 and monitored using tshark files.

Figure 1 shows the throughput performance of the network at different source data rates in the presence of 40 per cent blackhole and greyhole nodes. It is seen that the AODV with trust offers 76 per cent throughput in the presence of 40 per cent blackhole and greyhole nodes. The ad hoc nodes monitor their neighbours and accordingly chose a best trusted neighbour for forwarding their data. The loss of 25 per cent in trusted AODV is due to the time taken by the neighbouring nodes to learn about the malicious behaviour of its neighbour. The average end-to-end delay of AODV with trust is more than default AODV by 0.1ms as shown in Fig. 2. This is the overhead associated with the trust computation algorithm. Figure 3 shows the throughput varying the number of malicious nodes which launch flooding attack. The source is sending data at a rate of 15 packets/s and the malicious nodes are made to send RREQ packets to unknown destinations at 5 packets/s. The VAR trust

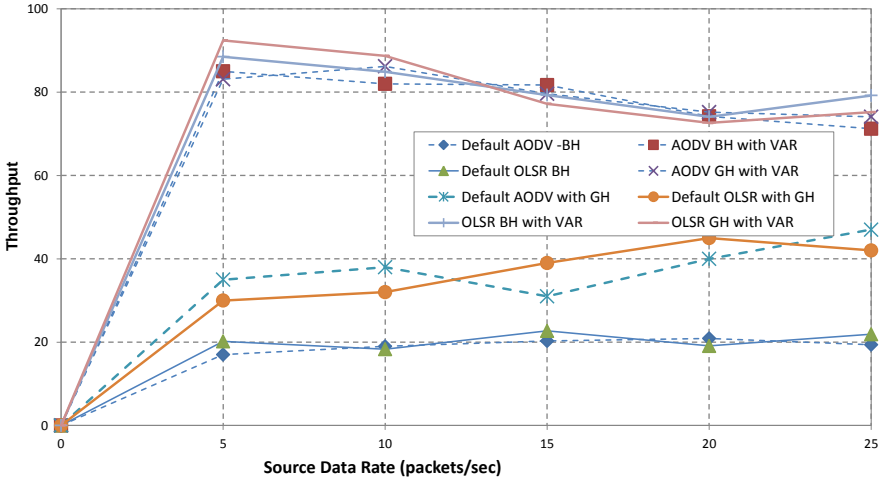

Figure 1. Comparison of the throughput by varying the source data transmission rate amidst 40 per cent blackhole (BH) nodes and 40 per cent greyhole (GH) nodes for the default protocols and customised VAR trust based routing protocols.

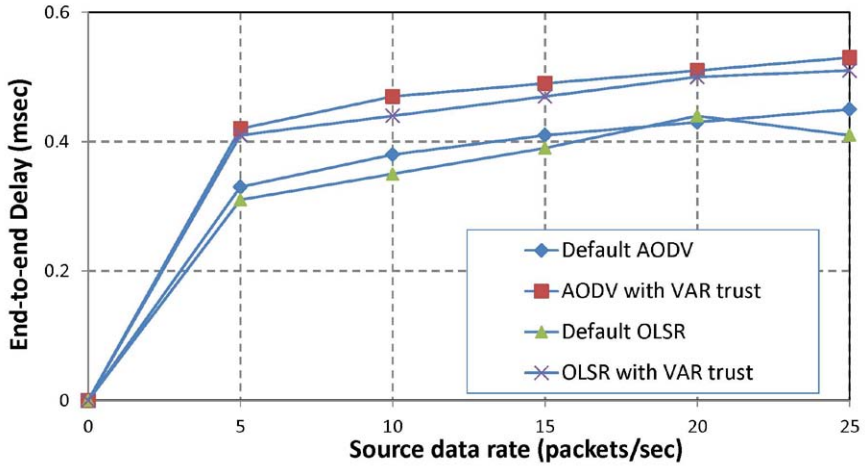

Figure 2. Comparison of end-to-end packet delay experienced by the packets in default and VAR trust-based routing protocols at different source data rates.

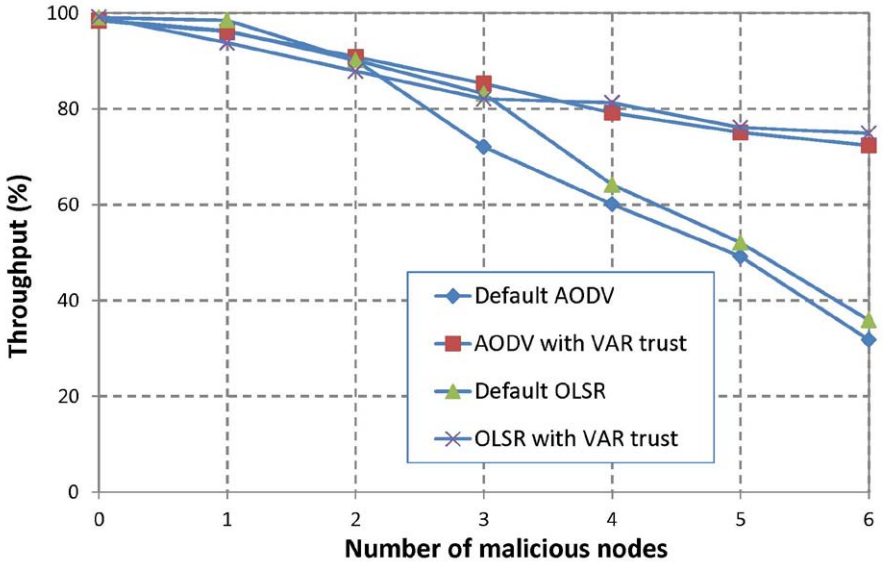

Figure 3. Comparison of the throughput against number of malicious nodes indulged in flooding attacks in the ad hoc testbed of 15 nodes.

model is able to easily identify these malicious behaviours and the data packets are effectively rerouted through trustworthy neighbours.

4.2 Performance of OLSR

The OLSR daemon is executed in the laptops participating in the ad hoc network. Through the front end interface, the laptops are configured for experimentation as specified in Table 2. Figure 1 shows the throughput of the network at various data rates in the presence of 40 per cent malicious nodes. The OLSR with trust maintains the throughput at 75 per cent. Figure 2 shows the end-to-end delay experienced by the data packets in the network. The average end-to-end delay in OLSR with trust is slightly higher than that of default OLSR by 0.09 ms.

4.3 Performance of the VAR Trust Model

The authors simulate the VAR trust model using the OPNET simulator and compare the proposed model with SRAC[4] and SLSP[8] with SMT[9] by various performance metrics. Table 3 lists the security attacks addressed by VAR model and SRAC in a reactive ad hoc routing scenario. Table 4 shows the false alarm rates for various trust models. It can be clearly seen that VAR model is able to quickly detect malicious nodes and the false alarm rates are minimal when compared to SRAC and SLSP/SMT.

Figure 4 shows the simulation results of trust overheads in computational time units for various trust models. SRAC incurs the maximum overhead due to the execution of encryption and decryption algorithms. This is especially significant in networks with high levels of mobility. It is shown that the overhead of SRAC is three times that of the VAR model for node speeds higher than 20 m/s. In SLSP, the overhead is due to securing the links and is approximately two times higher than the overheads in the VAR model. This is due to the use of the digital signature and authentication using hash chains.

The average time taken to detect a malicious neighbour in an ad hoc network is shown by the simulation results in Fig. 5. The simulation setup consists of 50 nodes spread over an area of 1000 m^2. Malicious nodes include black holes, grey holes and those indulging in flooding attacks and content modification attacks. These nodes are capable of launching multiple attacks at different time intervals. They constitute 40 per cent of the nodes in the network. It was found that VAR model is able to identify these attacks in 4.18 ms when the maximum node speed is 10 m/s. SRAC takes around 6 ms and this is due to the fact that the trust evaluations are based on one

Table 3. Handling security attacks in VAR and SRAC trust models

Security attacks	VAR trust metrics	SRAC
Dropping of control and data packets	T[1], T[2], T[5], T[6], T[7], T[8]	Detected indirectly by unsuccessful transmission counts of routing and data packets
Flooding the victim node with control and data packets	T[1], T[6], T[8]	Not detected
Non-cooperation in routing	T[1], T[2], T[3], T[4]	Detected by unsuccessful transmission counts of routing packets
Modification of messages by tampering with header/data	T[5], T[9]	All messages are encrypted. Header modifications are detected by unsuccessful transmission counts by the sender. Data packet modifications are not detected
Advertisement of false routes	T[3], T[4]	Detected by unsuccessful transmission counts of routing packets
Misrouting the data packets	T[5], T[9]	Perceived as loss of data packets

Table 4. Performance comparison with existing trust models

False alarms	Node speed (m/s)	VAR (ms)	SRAC (ms)	SLSP / SMT (ms)
False positive rate	5	0.13	0.22	0.18
	10	0.17	0.21	0.19
	15	0.17	0.22	0.21
	20	0.19	0.25	0.22
False negative rate	5	0.15	0.21	0.22
	10	0.16	0.23	0.21
	15	0.18	0.23	0.22
	20	0.18	0.26	0.24

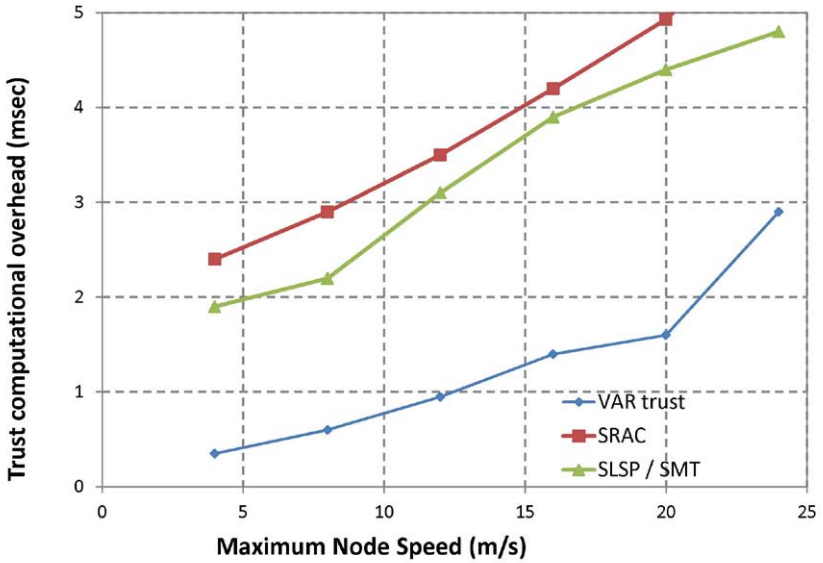

Figure 4. Average trust computational overhead varying the node speed in an ad hoc network of 15 nodes.

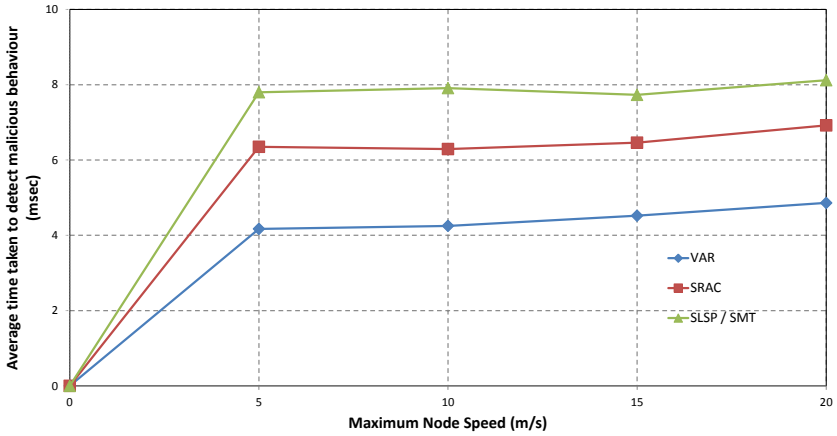

Figure 5. Average time taken to detect malicious behaviour in an ad hoc network of 50 nodes.

malicious activity, namely, non-forwarding of packets. Also, SRAC is unable to detect flooding attacks in the network. SLSP combined with SMT ensures secure link updates and robust data transfer via redundant message transmissions. It is able to detect few attacks like masquerading, due to neighbour lookup protocol's duplicate MAC address detection functionality. But, it fails to detect legitimate nodes that behave maliciously by launching multiple attacks at different intervals of time.

The space complexity of the VAR based trust is estimated to be $O(kn^3)$ where k is the number of sample data collected for trust analysis and n is the number of trust metrics to be evaluated.

5. CONCLUSIONS

A regression based trust model is implemented in a proactive and a reactive routing protocol and tested it over an ad hoc testbed. It was found that both AODV and OLSR fortified with the trust model show a throughput of at least 75 per cent amidst 40 per cent compromised nodes with the end-to-end packet delay higher by 0.1msec than the default protocols. It is shown that a generalized trust model can be easily incorporated over proactive and reactive ad hoc routing protocols and its performance can be studied in a realistic wireless scenario. The VAR trust model is able to identify multiple security attacks and performs better compared to the existing trust models.

Some of the future extensions to be pursued are the inclusion of recommendation trust and confidence parameter in the VAR trust model. Other interesting extensions include studying the overheads associated with the information exchange in the network due to propagation of trust, incorporation of other security attacks into the VAR trust model. The performance of this trust model over other ad hoc routing protocols and scalability issues concerned with the large scale deployment of ad hoc nodes in application specific scenarios are other areas to be pursued. Integration of trust based cognitive approaches to theoretical models in wireless security is also planned to be investigated in future.

ACKNOWLEDGMENTS

The authors thank the Defence Research Development

Organisation for providing the funding in executing this research work under Grant No.: IP/ER/0803748/M/01/1189. The authors also thank Chandrakanth Gaurav, Dhivya C. & Rashda Khanam of CSE Dept, SRM University for their help in conducting experiments on the testbed.

REFERENCES

1. Sivaram Murthy, C. & Manoj, B.S. Ad hoc wireless networks. Pearson Education, 2001. 20 p.
2. Butty´an, L. & Hubaux, J.P. Security and co-operation in wireless networks. Cambridge University Press, 2007. 30 p.
3. Pirzada, A.A.; Datta, A. & McDonald, C. Incorporating trust and reputation in DSR protocol for dependable routing. *Computer Communications*, 2006, **29**(15), 2806-21.
4. Yu, M.; Zhou, M. & Su, W. A secure routing protocol against Byzantine Attacks for MANETs in adversarial environments. *IEEE Trans. Veh. Technol.*, 2009, **58**(1), 449-60.
5. Velloso, P.B.; Laufer, R.P.; Cunha, D.O.; Duarte, O.C.M.B. & Pujolle, G. Trust management in mobile ad hoc networks using a scalable maturity-based model. *IEEE Trans. Netw. Serv. Management.*, 2010, **7**(3), 172-85.
6. Theodorakopoulos, G. & Baras, J.S. On trust models and trust evaluation metrics for ad hoc networks. *IEEE J. Sel. Areas Commun.*, 2006, **24**(2), 318–28.
7. Zapata, M.G. Secure ad hoc on-demand distance vector routing. *ACM Mobile Comput. Commun. Rev.*, 2002, **6**(3), 106-07.
8. Papadimitratos, P. & Haas, Z.J. Secure link state routing for mobile ad hoc networks. *In* Proceedings of the IEEE CS Workshop on Security and Assurance in Ad hoc Networks, Orlando, FL, Jan 2003. pp. 379-83.
9. Papadimitratos, P. & Haas, Z.J. Secure data communication in mobile ad hoc networks. *IEEE J. Sel. Areas Commun.*, 2006, **24**(2), 343-56.
10. Conti, M. & Giordano, S. Multihop ad hoc networking: The reality. *IEEE Commun. Mag., 2007,* **45**(4), 88-95.
11. Burbank, J.L.; Chimento, P.F.; Haberman, B.K. & Kasch, W.T. Key Challenges of military tactical networking and the elusive promise of MANET technology. *IEEE Commun. Mag.*, 2006, **44**(11), 39-45.
12. Chang, B.-J. & Kuo, S.-J. Markov chain trust model for trust-value analysis and key management in distributed multicast MANETs. *IEEE Trans. Veh. Technol.*, 2009, **58**(4), 1846-863.
13. Perrig, A.; Szewczyk, R.; Wen, V.; Culler, D. & Tygar, J. SPINS: Security protocols for sensor networks. *In* Proceedings of ACM Mobile Computing and Networking (MobiCom), Rome, Italy, 2001. pp. 189-99.
14. Zhu, S.; Setia, S. & Jajodia, S. LEAP: Efficient security mechanisms for large scale distributed sensor networks. *In* Proceedings of 10th ACM Conference on Computer and Communications Security, New York, 2003. pp. 62-72.
15. Boukerch, A.; Xu, L. & El-Khatib, K. Trust-based security for wireless ad hoc and sensor networks. *Computer Communications*, 2007, **30**(11-12), 2413-427.
16. Bedi, P.; Sinha, A.K.; Agarwal, S.; Awasthi, A.; Prasad, G. & Saini, D. Influence of terrain on modern tactical combat: Trust-based recommender system. *Def. Sci. J.*, 2010, **60**(4), 405-11.
17. Wang, K. & Wu, M. Co-operative communications based on trust model for mobile ad hoc networks. *IET Inf. Secur.,* 2010, **4**(2), 68-79.
18. Biller, B. & Nelson, B.L. Modeling and Generating Multivariate Time-series input processes using a vector autoregressive technique. *ACM Trans. on Model. Comput. Simul*. 2003, **13**(3), 211-37.
19. Gujarati, D.N. Basic econometrics, McGraw-Hill/Irvin, 2003. 302 p.
20. Uppsala University, http://apetestbed.sourceforge.net/. [Accessed on 16 January 2012].

Contributors

Ms Revathi Venkataraman is pursuing her PhD. Currently working as Assistant Professor in the Department of Computer Science and Engineering, SRM University. Her other research interests are wireless ad hoc and sensor network testbed developments which are ongoing research activities funded by Indian Government. Her research interests include wireless networks and security, trust computing and routing in ad hoc networks.

Dr T. Rama Rao received his PhD from Sri Venkateswara University, Tirupati, India in the year 2000. Currently, working as 'Professor & Head', Department of Telecommunication Engineering, Faculty of Engineering & Technology, SRM University, India. His research interests include: Radio channel measurements and modeling, broadband wireless communications/networks and wireless information networks.