Title : Implementation of a Regression based trust model in a Wireless ad hoc Testbed

Abstract: Wireless ad hoc networks are resource constraint and vulnerable to various security attacks. Trust based security modeling 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 (AODV) protocol and Optimized Link State Routing (OLSR) protocol and compared the performance of these protocols amidst malicious compromised nodes in a wireless ad hoc testbed. The experimental results show the feasibility of implementing trust models over real ad hoc network deployments. Our simulations results show that the proposed VAR trust model offers better performance compared to the existing trust models.

Keywords: Trusted AODV, Trusted OLSR, Vector Auto Regression Trust, Econometric Trust Model.

Table 1 : Generalized Trust metrics for ad hoc routing

TABLE 1

|  |  |  |
| --- | --- | --- |
| 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 neighbor | Number of RREQs received from the neighboring node |
| *T[3]* | Number of occurrences showing the neighbor willingness to participate in data communication | Number of RREPs received from the neighbor |
| *T[4]* | Number of occurrences the neighbor is chosen as an MPR | Time taken to respond to a RREQ message. |
| *T[5]* | Number of DATA packets successfully forwarded by neighbor | |
| T[6] | Number of DATA packets received from the  neighbor | |
| T[7] | Number of ACKs forwarded by the neighbor | |
| *T[8]*  *T[9]* | Number of ACKs received from the neighbor  Number of DATA packets forwarded without content modification | |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

No vertical lines in table. Statements that serve as captions for the entire table do not need footnote letters.

aGaussian units are the same as cgs emu for magnetostatics; Mx = maxwell, G = gauss, Oe = oersted; Wb = weber, V = volt, s = second, T = tesla, m = meter, A = ampere, J = joule, kg = kilogram, H = henry.

Table 2: Experimental Setup Parameters

|  |  |
| --- | --- |
| Parameter | Value |
| Experimental Area | 600 × 600 m2 |
| Maximum node speed | 20 metres per second |
| α | 0.5 |
| Transmission Range (Indoors) | 70 metres (approximately) |
| Number of Nodes | 15 |
| Data packet Size | 50 bits |
| Duration of Experimentation | 30 minutes |
| Channel Data Rate | 11 Mbps |
| VAR time lag (*p*) | 2 |
| Number of trust metrics evaluated | 8 |

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Performance Metrics** | **Node speed (m/s)** | **VAR**  **(msec)** | **SRAC**  **(msec)** | **SLSP / SMT**  **(msec)** |
| Average time taken to detect malicious behavior | 5 | 4.17 | 6.35 | 7.8 |
| 10 | 4.25 | 6.29 | 7.91 |
| 15 | 4.52 | 6.46 | 7.73 |
| 20 | 4.86 | 6.92 | 8.12 |
| 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 |

C:\Users\revathi\Desktop\def scien journal\fig1.tif

Fig. 1. Comparison of the throughput by varying the source data transmission rate amidst 40% blackhole nodes for the default protocols and customized VAR trust based routing protocols.

C:\Users\revathi\Desktop\def scien journal\fig3.tif

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

C:\Users\revathi\Desktop\def scien journal\fig2.tif

Fig. 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.

C:\Users\revathi\Desktop\def scien journal\fig4.tif

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

Fig. 1. Comparison of the throughput by varying the source data transmission rate amidst 40% blackhole nodes for the default protocols and customized VAR trust based routing protocols.

Fig. 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.

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

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

C:\Users\revathi\Desktop\photos\revathi (2).tifRevathi Venkataraman is doing her PhD and working as Assistant Professor in the Department of Computer Science and Engineering, SRM University. Her research interests include wireless networks and security, trust computing and routing in ad hoc networks. She was a visiting research faculty at the Electrical Engg dept, Viterbi School of Engineering, University of Southern California for a duration of six months. Her other research interests are wireless ad hoc and sensor network testbed developments which are ongoing research activities funded by Indian Government.

C:\Users\revathi\Desktop\photos\rr (2).tifT. Rama Rao currently, working as ‘Professor & Head’, Department of Telecommunication Engineering, Faculty of Engineering & Technology, SRM University, India. He received his PhD degree on ‘Radio Wave Propagation studies for Fixed and Mobile Communications over Southern India’ from Sri Venkateswara University, Tirupati, India in the year 2000. He worked with Aalborg University, Denmark as ‘Assistant Research Professor’; with Universidad Carlos III de Madrid, Spain and at the University of Sydney, Australia as ‘Visiting Professor’. He served as a ‘PostDoc Research Fellow’ at National Chio Tung Univeristy, Hsinchu, Taiwan. He has a long-standing research history on Radiowave Propagation Studies for Wireless Communications. His research interests are, Radio Channel Measurements & Modeling, Broadband Wireless Communications/Networks and Wireless Information Networks.

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. 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.
4. Velloso, P.B. *et al*. Trust management in mobile ad hoc networks using a scalable maturity-based model. *IEEE Trans. Netw. Service Management*, 2010, 7(3), 172-185.
5. Pirzada, A.A.; Datta, A. & McDonald, C. Incorporating Trust and Reputation in DSR protocol for dependable routing*. Computer Communications*, 2006, 29(15), 2806-21.
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. Review*, 2002, 6(3), 106-107.
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. Magazine, 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. Magazine*, 2006, 44(11), 39-45.
12. Uppsala University, <http://apetestbed.sourceforge.net/>. [Accessed on 16 January 2012]
13. Gujarati, D.N. Basic Econometrics, McGraw-Hill/Irvin, 2003. 302 p.