ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 1, Issue 8, October 2012

Comparative Study and Analysis of Soft Computing Techniques Implemented in Secure Data Transmission

Hemant Kumar Garg, P.C.Gupta

Abstract-Data transmission in the wireless network is very big challenge. Several factors affect to transmit data safely. In this paper we have identified possible reasons which can affect the transmission of data. We have also shown how soft computing techniques can be helpful in secure data transmission.

Keywords- Soft Computing; Ad hoc network; Threat; Attacks.

1. Introduction

Any system that has to be protected might have weaknesses or vulnerabilities, some or all may be targeted by an attacker. One approach of designing security mechanisms for systems is to look at the threats that the system faces and the attacks possible given the vulnerabilities. The designed security mechanisms should then ensure that the system is secure in the light of these threats, attacks, and vulnerabilities. Another problem with defending wireless ad hoc networks is that existing security technologies are more geared towards wire line networks, which are fairly static. Existing technologies often rely on the availability of traffic choke points (which most traffic goes through). Security devices placed at such choke points can inspect traffic for suspicious behavior and implement security policies and respond as needed. This is not true in ad hoc networks where the network entities often move around. This results in frequent changes in the structure of the network. Traditional security solutions also depend on a few centrally located devices for managing the security of the network. Such solutions are not applicable for wireless ad hoc networks on account of the features of these networks.

2. Literature Survey

Different work has been already done in the implementation of secure data transmission through soft computing techniques in Ad hoc networks. In one work, to improve the more security in data transmission updating techniques have been implemented. In this algorithm the work was to solve the session hijacking, traffic analysis and eavesdropping, higher level attacks, operating system bugs and different type of security methods like treat base stations as entrusted and setting up a virtual private network [1].

In another work a method has been used to support high data transmission rate in ad hoc network based on blue tooth. In this work the new network topology called "DoublePico" (Double Piconet) for overcoming low data transmission rate was proposed in a scatternet which was constructed by Bluetooth piconets. To construct the DoublePico, the node, which performs the function of the relay station, has two blue tooth devices. Two different piconets were linked in one node by the link with the two blue tooth devices, thereby forming the ad hoc networks [2].

In another work a method was proposed based on percolation for the machine-to machine stub network. A new routing and data transmission method for the stub network was based on the six degrees of separation. The scheme consists of two phases: routing phase and the data transmission phase. In the probe phase, probes packets are transmitted and are flowed in the network [3].

One more work, states about different wireless network security techniques. Security techniques whose results confirm an intuitive claims: the more attackers there are in the network, more damaging they inflict in to a multicast session in terms of packet delivery ratio, hence it's better to remove such nodes from the network altogether.

The next section describes possible threats which can affect the performance of the data transmission.

3. Threats affect data transmission

Threat is the means through which the ability or intent of an agent to adversely affect an automated system, facility or operation can be manifested. All methods or things used to exploit a weakness in a system, operation, or facility constitute threat agents [4]. Examples of threats include hackers, disgruntled employees, industrial espionage, national intelligence

***Hemant Kumar Garg**, Government Women Polytechnic College, Gandhi Nagar, Jaipur, INDIA,(hg_avi@rediffmail.com).*
***P.C.Gupta**, University of Kota, Kota, INDIA, (gupta.pc26@gmail.com).*

services, and criminal organizations. In the following sections some of the possible threats have been explained:

3.1 Vulnerability

It is any hardware, firmware, or software flaw that leaves an information system open for potential exploitation. The exploitation can be of various types, such as gaining unauthorized access to information or disrupting critical processing.

3.2 Attack

It is an attempt to bypass the security controls on a computer. The attack may alter, release, or deny data. The success of an attack depends on the vulnerability of the system and the effectiveness of existing counter measures. Examples of attacks include actions such as stealing data from storage media and devices, obtaining illegitimate privileges, inserting data falsely, modifying information, analyzing network traffic, obtaining illegitimate access to systems through social engineering, or disrupting network operation using malicious software [5]. Attacks can be divided into two main categories:

- **Passive attacks**

In these types of attack an attacker passively listens to the packet or frame exchanges in the wireless medium by sniffing the airwaves. Since an attacker only listens to the packets that are passing by without modifying or tampering with the packets, these attacks mainly target the confidentiality attribute of the system. However, this process of gathering information might lead to active attacks later on. Typically this attack is easier to launch than the next type of attacks.

- **Active attacks**

Active attacks are those attacks where the attacker takes malicious action in addition to passively listening to on-going traffic. For example an attacker might choose to modify packets, inject packets, or even disrupt network services. Security in wireless networks differs markedly from security for their wire line counterparts due to the very nature of the physical medium. While communicating over a wireless medium, the transmitted and received signals travel over the air. Hence, any node that resides in the transmission range of the sender and knows the operating frequency and other physical layer attributes (modulation, coding, etc.) can potentially decode the signal without the sender or the intended receiver knowing about such an interception.

4. Comparative Analysis of Implementation of Soft computing Techniques in Secure Data Transmission

Table: Five research papers have been used for the analysis of the work in which soft computing techniques have been implemented:

	I	II	III	IV	V
Purpose	Study of two routing attacks which use non-cooperative network members and disguised packet losses to develop adhoc network resources and to reduce adhoc routing performances [21].	In some problems which occurred for the period of information transmitting like session hijacking, MAC spoofing etc [1].	To implement a successful e-Government application in which security was required [24].	It highlights the challenges posed by the need for security during system architecture design for wireless devices [25].	To develop a simple, efficient and secure multicast protocol [23].
Approach Applied	Configuring and reconfiguring self-healing communities for each end to end connection, a chain of self-healing communities along the shortest path are established to route disruption.	Different types of security methods like Treat base stations, setting up a virtual private network etc.	Web Application Firewall (WAF), which is called (HiWAF), is a web application firewall that works in three modes: positive, negative and session based security mode.	Cryptographic algorithms, security enhancement to embedded processors, and advanced system architecture for wireless devices.	Implemented a prototype system which validates secure multicast protocol and evaluates against various performance matrices.
Result	It verifies that it is effective and efficient to use paradigm to secure common ad hoc routing protocols.	The best course of action for network engineers is to assume that the link layer offers no security.	It gives the brief summary of the current security solutions that are currently available to secure e-Government web application.	Security considerations will become an integral part of system design for wireless handsets, rather than being addressed as an afterthought.	Video-on-Demand application are even better and show that if we perform copy right protection of video data off-line, our protocol can successfully multicast video security and with copy-right protection.

Conclusion	In this paper it has shown that how non-cooperative members can threat the secure routing protocols by various means. Particularly, they can deplete network resources and reduce the routing performance to minimum.	The protocols are evolving to meet the needs of serious users. Treat wireless stations as you would treat an unknown user asking for access to network resources over a untrusted network.	The hybrid web application firewall is the first security solution that applied both ANN & Fuzzy logic concepts.	A new security protocols optimized for the wireless environment, new system architectures and system design methodologies.	It presents a secure multicast protocol with two components: the key distribution protocols & secure multicast watermark protocol.

5. Conclusion

In this paper different factors are identified which can affect the transmission of the data. After an in-depth review it has been found that very few work have been done so far in which the concept of soft computing techniques are implemented to transmit the data safely. Hybrid web application firewall is the first security solution in which both ANN & Fuzzy logic have been applied. This opens the gate of soft computing as an approach which in the future can be utilized in secure data transmission.

6. References

[1] R.Seshadri and N.Penchalaiah “Improving the more security in data transmission by using dynamic key and router updating techniques”.

[2] Byoung Kug Kim, Sung Hwa Hong “A Method to Support High Data Transmission Rate in Ad hoc Networks based on Bluetooth”.

[3] Xiangming Li, Jihua Lu “A Novel Routing and Data Transmission Method for Stub Network of Internet of Things based on Percolation.”

[4] F. Stajano and R. Anderson, “The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks,” in Proceedings of 7th International Workshop on Security Protocols, Cambridge. Picture Notes in Computer Science, Vol. 1396, Springer, Berlin 1999, pp. 132–194.

[5] J. Douceur, “The Sybil Attack,” in Proceedings of IPTPS 2002, March 2002, Cambridge, MA, pp. 251–260.

[6] A. Sabir, S. Murphy, and Y. Yang, “Generic Threats to Routing Protocols,”draft-ietf-rpsec-routing-threats-07, October 2004.

[7] C.-Y. Tseng, P. Balasubramanyam, C. Ko, R. Limprasittiporn, J. Rowe, and K. Levitt, “A Specification-Based Intrusion Detection System For AODV,” in Workshop on Security in Ad Hoc and Sensor Networks (SASN)’03.

[8] G. Vigna, S. Gwalani, K. Srinivasan, E. Belding-Royer, and R. Kemmerer, “An Intrusion Detection Tool for AODV-based Ad hoc Wireless Networks,” in Proceedings of the Annual Computer Security Applications Conference (ACSAC), Tucson, AZ, December, 2004, pp. 16–27.

[9] P. Ning and K. Sun, “How to Misuse AODV: a Case Study of Insider Attacks against Mobile Ad-hoc Routing Protocols,” in Proceedings of the 2003 IEEE Workshop on Information Assurance. United States Military Academy, West Point, NY, June 2003.

[10] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, Handbook of Applied Cryptography, CRC Press, October 1996.

[11] J. Walker, “Unsafe at any Key Size; an Analysis of the WEP Encapsulation,” IEEE P802.11, Wireless LANs, October 2000.

[12] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. D. Tygar, “SPINS: Security Protocols for Sensor Networks,” Wireless Networks Journal (WINE), September 2002.

[13] L. Eschenauer and V. Gligor, “A Key-management Scheme for Distributed Sensor Networks.” In Proceedings of the 9th ACM Conference on Computer and Communications Security, November 2002, pp. 41–47.

[14] L. Zhou and Z. Haas, “Securing Ad Hoc Networks,” IEEE Network, 13(6), 24–30 (1999).

[15] H. Luo, J. Kong, P. Zerfos, S. Lu, and L. Zhang, “URSA: Ubiquitous and Robust Access Control for Mobile Ad Hoc Networks,” IEEE/ACM Transactions on Networking, December 2004, pp. 1049–1063.

[16] J. Kong, P. Zerfos, H. Luo, S. Lu, and L. Zhang, “Providing Robust and Ubiquitous Security Support for Mobile Ad Hoc Networks,” in Proceedings of Ninth International Conference on Network Protocols (ICNP), November 2001.

[17] S. Capkun, L. Buttyan, and J.-P.Hubaux, “Self-Organized Public-Key Management forMobile Ad Hoc Networks,” IEEE Transactions on Mobile Computing, 2(1), 52–64 (2003).

[18] J.-P. Hubaux, L. Butty´an, and S. Capkun, “The Quest for Security in Mobile Ad hocNetworks,” in MobiHoc. ACM, New York, 2001, pp. 146–155.

[19] S. Basagni, K. Herrin, D. Bruschi, and E. Rosti, “Secure Pebblenet,” in Proceedings of the 2001

ACM International Symposium on Mobile Ad Hoc Networking and Computing, MobiHoc 2001, Long Beach, CA, 4–5 October 2001, pp. 156–163.

[20] S. Zhu, S. Setia, and S. Jajodia. "LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks," in Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS '03), Washington, DC, October 2003.

[21] Jiejun Kong, and Xiaoyan, (May, 2005), "A secure Adhoc Routing Approach using Localized Self-healing Communities".

[22] H. Chan, A. Perrig, and D. Song, "Random Key Predistribution Schemes for Sensor Networks", in IEEE Symposium on Security and Privacy, May 2003, pp. 197–213.

[23] Hao-Hua Chu, LintianQiao, (April, 2002), "A secure multicast protocol with copyright protection".

[24] Asaad Moosa and EanasMuhsen Alsaffar, (2008), "Proposing a Hybrid-Intelligent framework to secure e-Government Web Applications".

[25] Srivaths Ravi and Anand Raghunathan, (Oct., 2002), Securing Wireless Data: System Architecture Challenges".

Er. Hemant Kumar Garg received the Bachelors degree in Computer Engineering from the University of Amravti of Amravati , India in 1991, and the M.Tech. Degree in Computer Science from the BIT, Ranchi, India in 2002, and is currently pursuing the Ph.D. degree in Computer Science & Engineering at JNU, Jaipur, India. In 1994, he joined the Computer Engineering Department, Department of Technical Education, Govt. of Rajasthan, Rajasthan State, INDIA, where he is currently working as a Lecturer (Selection Scale). He published a book on "Electronic Communication and Data Communication". **Er. Garg** is a Member of Institution of Engineers, India. He also has many publications in National and International Journals. His areas of interests include Ad Hoc networking and its Applications.

Dr. P.C. Gupta received Ph.D Computer Science from Bundelkhand University, Jhansi. He is working as Associate Professor, Department of Computer Science & Informatics, University of Kota, Kota, Rajasthan, IINDIA. He is guiding a number of Ph.D. Research Scholars. He has published various research papers in National and International Conferences and Journals. His research interest lies in Artificial Intelligence and Neural Networks.