Adaptive Security Framework for Ad-Hoc Mobile Wireless Network

RAJANI MURALEEDHARAN & LISA ANN OSADCIW PhD,
L.C. SMITH COLLEGE OF ENGINEERING, SYRACUSE UNIVERSITY, SYRACUSE, NY.

Goal

- To analyze and propose a defense mechanism against cross layer Denial of Service (DoS) attacks in Ad-Hoc Wireless Networks (AWN).
- To predict the validity of the DoS attacks using receiver operating characteristics (ROC).
- To achieve maximum reliability on DoS claims improving the Quality of Service (QoS) using evolutionary algorithms (Ant System).

Swarm Intelligence (Ant System)

- Multiple ants (agents) working together to find the global optimum.
- Communicate interactively either directly or indirectly.
- Move towards optimal solution by sharing knowledge.
- Depositing pheromones for communication.
- Tabu-list serves as a memory tool.

Application Layer	"Traditionally, communication using AWN is assumed to be SECURE"
Presentation Layer	
Session Layer	
Transport Layer	*Protocol (Flooding, De-synchronization)*
Network Layer	*Routing (Misdirection, Homing, Black Hole)*
Data Link Layer	*Coding (Collision, Exhaustion, Unfairness)*
Physical Layer	*Modulation (JAMMING)*

Mathematical Approach

Initializing of AWN:

$D_{xy} = \text{sqrt}((X_1-X_2)^2 + (Y_1 - Y_2)^2)$

$\psi_{ij} = 10$

Global Performance, η_{ij}, =

$$\frac{w_1*(H_p - H_a)}{H_p} + \frac{w_2*(D_p - D_a)}{D_p} + \frac{w_3*(E_p - E_a)}{E_p}$$

DoS parameters

$$+ \frac{W_4*(PD_p - PD_a)}{PD_p} + \frac{W_5*(PL_p - PL_a)}{PL_p} + \frac{W_6*(B_p - B_a)}{B_p} + \frac{W_7*(SNR_p - SNR_a)}{SNR_p}$$

Transition Probability P_{ij},

$$P_{ij} = \frac{[(\psi_{ij})^{\alpha} .(\eta_{ij})^{\beta}]}{\Sigma_k [(\psi_{ik})^{\alpha} .(\eta_{ij})^{\beta}]}$$

For Number of Iterations

1. $E_{ij} = 1/ (D_{ij})^2$
2. Pheromone deposition ψ_{ij} (t) = ρ ψ_{ij} (t-1) + Q/η_t
3. transition probability,
4. Update Tabu List

Results & Analysis

Jammer Type	# of Malicious nodes	Average Distance	Average Energy	Average Packet Loss	Average Packet Delivery	Detection (%)
STJ	3	9.756	15.2038	0.038	97.349	0.9721
	12	92.373	50.0292	0.3792	68.7423	0.8619
ELINT	3	10.2921	20.948	0.173	82.1823	0.8023
	12	70.0383	90.893	0.9236	0.0034	0.5466
Sybil Attack	3	11.0972	12.2241	0.0212	85.0068	0.8197
	12	67.4066	80.4509	0.5731	25.7913	0.6063
Worm-hole Attack	3	6.0793	29.2943	0.0167	92.1670	0.8594
	12	50.4687	75.9057	0.1905	37.4319	0.7089

Conclusion

- Under Single Tone Jammer (STJ) attack, 97% packet delivery is achieved.
- Under ELINT attack, 82% packet delivery with only 20% energy dissipation is obtained.
- Under Sybil attack, 97% of the time illegitimate nodes were detected prior to attack.
- Collision in Ant System was avoided by 93%, under 50% of network failure.
- Trade-off between performance parameters such as energy, Pd, Pl and DoS characteristics is dependent on the Weights.
- Addition of parameters in the future will not affect the approach.