ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)
Vol. 4, Issue 3 (Jul. - Sept. 2016)
International Journal of Advanced Research in Computer Science & Technology (IJARCST 2016)

Genetic Based Ant Colony Optimization Algorithm to Optimize Wireless Sensor Network

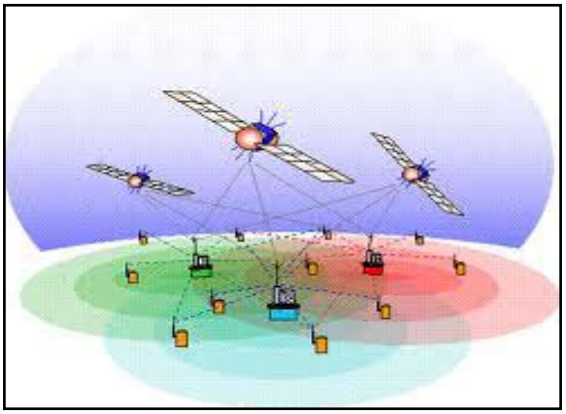
[I]Pooja, [II]Er. Kapil Arora
[I]M.Tech(Student), [II]Assistant Professor
[I,II]Dept. of ECE, RPIIT College, Karnal, Haryana, India

Abstract
Wireless sensor networks that are deployed in applications such as battlefield monitoring and home sentry systems face acute security concerns, including eavesdropping, forgery of sensor data, denial of service attacks, and the physical compromise of sensor nodes. Sensor networks are often organized hierarchically, with a base station serving as a gateway for collecting data from a multi-hop network of resource-constrained sensor nodes. Prior work that has focused on securing the routing between sensor nodes has assumed that the base station is sufficiently powerful to defend itself against security threats. This paper considers strategies for securing the sensor network against a variety of threats that can lead to the failure of the base station, which represents a central point of failure. Intrusion detection system in wireless sensor network is one of the Growing research areas in recent years. Wireless sensor networks (WSN) consist of tiny devices. These tiny devices have limited energy, computational power, transmission range and memory. However, wireless sensor networks are deployed mostly in open and unguarded environment. Therefore, intrusion detection is one of the important aspects for wireless sensor networks. Here are two different kind of intrusion detection mechanism: anomaly based and signature based. In this paper, we mention several attacks on WSN and we primarily focus only on the anomaly based intrusion detection system. Finally, we discuss about several existing approaches to describe how they have identified security threats and implemented their intrusion detection system.

Keywords
WSN, DOS, sensor network, attacks, GA

I. Introduction

Wireless sensor networks are rapidly growing in popularity. Applications of sensor networks that have emerged include habitat monitoring [1], robotic toys [2], and battlefield monitoring [3]. A wide range of applications are emerging, including location aware sensor networks in the home and office, assistive technology for biomedical sensing, and outdoor deployments of sensor networks to monitor storms, oceans, and weather events. For military deployments, security is essential to protect the routing infrastructure and packet data from threats such as eavesdropping, tampering, denial-of-service (DOS) attacks, and the physical compromise of sensor nodes deployed into enemy territory.



The research challenge is to secure the routing infrastructure against such threats given the severe resource constraints imposed by wireless sensor networks. Wireless sensor networks consist of individual sensor nodes that are highly resource-constrained in terms of their limited energy lifetime, modest CPU, and scant memory [2, 8]. While it has been demonstrated that symmetric key cryptography can be implemented on today's wireless sensor platforms [5,12], initial results indicate that public key cryptography remains out of reach for today's sensor networks due the compute-intensive nature of public key methods [12]. Prior work in securing wireless sensor networks therefore focuses on exploiting symmetric key-based techniques for achieving authentication, data integrity, and confidentiality. As a result, a key focus of this paper concerns security obtained through symmetric key cryptography.

Routing protocols can also be classified in terms of an architectural view. The most traditional classification contains hierarchical protocols and flat protocols. A third classification identifies two types of mechanisms according to the location characteristic: Physical Location Information (PLI)-based protocols giving approximate location for mobile nodes, and PLI-less protocols. We note the diversity of the suggested approaches and the difficulty to conclude on the predominance of a specific protocol compared to the others. Recall that none of these protocols takes into account QoS parameters, security or multicast.

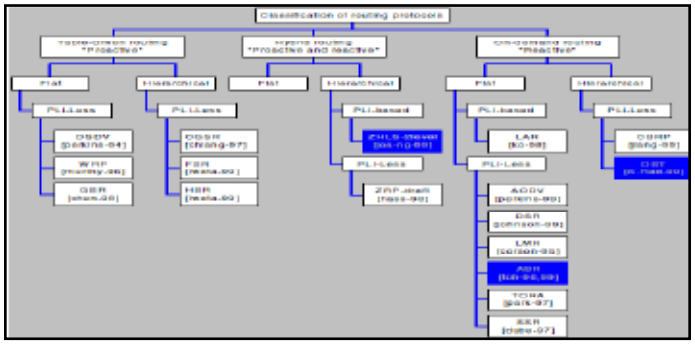


Fig. 1 : Classification of routing protocols

II. Multiple Base Stations: Route Discovery

A route discovery protocol ascertains the topology of the sensor network. Our route discovery protocol is based on INSENS route discovery protocol [12]. INSENS provides support for intrusion-tolerant routing in wireless sensor network. It builds multiple redundant paths between sensor nodes and a base station to bypass intermediate compromised nodes. In addition, INSENS

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

limits DOS-style flooding attacks, prevents false advertisement of routing and other control information, and is designed for resource-constrained wireless sensor network. In particular, INSENS ensures that a single compromised node can only disrupt a localized portion in the network, and cannot bring down the entire sensor network.

Route discovery is subdivided into two rounds. In the first round, the base station floods (limited flooding) a request message to all the reachable sensor nodes in the network. In the second round, each sensor node sends its neighborhood topology information back to two different base stations using a feedback message.

1. Route Discovery: Route Request

A malicious node in the network can attempt to launch several attacks in this round. First, it can attempt to spoof the base station by sending a spurious request message. Second, it can include a fake path in the request message it forwards. Third, it may not forward a request message, or launch a DOS attack by repeatedly sending several request messages. We adopt the security mechanisms of INSENS to counter these attacks. They require sensor nodes to be pre-configured with appropriate values.

The second mechanism that we use to defend against intrusions is a keyed MAC algorithm. Each sensor node is configured with a separate secret key that is shared only with the base station. This keyed MAC is used to preserve the integrity of control information included in a request message. The overall effect of these security mechanisms is that a malicious node can attack in the first round only by localized flooding, by not forwarding a request message, and by sending fake path in the request which is later on detected in the second round. The latter two attacks will result in some of the nodes downstream from the malicious node not getting a request message or not being able to forward their feedback message to the base station in the second round. Again, a malicious node may be able to compromise a small number of nodes in its vicinity by employing these types of attacks, but cannot jeopardize the security of the complete network.

2. Route Discovery: Route Feedback

In the second round, each sensor node sends its local connectivity information (a set of identities of its neighbor nodes as well as the path to itself from a base station b) back to the base station b using a feedback message. A separate feedback message is sent to every base station whose request message was forwarded in the first round. The mechanism used to send feedback messages to different base stations is same. So, for simplicity, we will concentrate on sending a feedback message to just one base station in the following discussion. After a node has forwarded its request message in round one, it waits a certain timeout interval before generating a feedback message. This interval allows a node to listen to the local broadcasts of its neighbors, who will also be forwarding the same request message. A node will hear the request messages from its upstream, peer and downstream neighbors. A feedback message containing neighbor list and path to b is propagated to b using the reverse path taken by the request message initiated by b.

The overall effect of these security mechanisms is that a malicious node is limited in the damage it can inflict, whether attacking by DOS attack, by not forwarding a feedback message or by modifying the neighborhood information of nodes, which can be detected at the base station. The rate-controlled DOS attack will affect upstream nodes, but only in a limited way. The latter two attacks will result in some of the nodes downstream from the malicious node not being able to provide their correct connectivity information to the base station. Though a malicious node could launch a battery-drain attack by persistently sending spurious feedback messages at the rate-controlled limit, such an attack would still affect a limited number of upstream nodes. In summary, a malicious node may be able compromise only a small number of nodes in its vicinity using these attacks.

IV. Multiple Base Stations: Multi-Path Data Routing

A common technique to tolerate failures and security compromises of intermediate nodes in a computer network is to build multiple redundant routing paths between source and destination nodes. These paths are independent of one another in the sense that they share as few common nodes/links as possible; ideally, only source and destination nodes are shared among different redundant paths. Each message sent from a source to a destination is sent multiple times, once along each redundant path. The presence of a few failed or compromised nodes along some of these paths can jeopardize the delivery of some of the copies of a message. However, as long as there is at least one path that does not contain a failed or compromised node, the destination is guaranteed to receive at least one copy of the message that has not been tampered with. An important advantage of this technique is that it does not require any need for detecting failures or intrusions, i.e. it works despite the presence of (undetected) intrusions. We exploit this technique to build multiple redundant paths in a wireless sensor network.

V. Simulation Results

The proposed work is about the generation of such an approach that will dynamically compensate the problem of link failure and provide the optimize solution without any data loss. The proposed system will give the benefit in terms of Efficiency and accuracy.

A. Scenario 1

Parameter
Value
Number of Nodes
10
Topography Dimension
100 m x 100 m
Traffic Type
CBR
Topology
Random
Initial Node
1
Destination Node
10

Simulation Parameters of Existing Work

Table1

Parameters	Values
Distance	49.54(meters)
Energy Consumed	6.5119e+003(joules)
Network Delay	1.4845e+005 ms

B. Proposed Appraoch

A form of knowledge representation suitable for notions that cannot be defined precisely, but which depends upon their contexts.

1. Traditional Approach

If slow speed =0 If fast speed= 1

2. Proposed Method

Every problem must represent in terms of fuzzy sets that is [0 1]
Slowest [0.0 – 0.25]
Slow [0.25 – 0.50]
Fast [0.50 – 0.75]
Fastest [0.75 – 1.00]

3. Advantages of Genetic concept

1. Premature convergence is a common problem in finding the optimal solution in Traditional Algorithms and it is strongly related to the loss of the population diversity.
2. When population diversity is low, a ACO will converge very quickly. On the Other hand, if the diversity of the population is too high, it is very time consuming for a PSO to converge and this may cause wastage in computational resources.

4. Simulation Parameters of Proposed work

Parameters	Values
Distance	10.15(meters)
Energy Consumed	2.2569e+3(joules)
Network Delay	1.8787e+003 ms

V. Conclusions

In this paper, we have addressed the issues securing a wireless sensor network against a variety of threats that can lead to the failure of the base station, which represents a central point of failure. First, multipath routing to multiple destination base stations is analyzed as a strategy to provide tolerance against individual base station attacks or sensor node compromises. Second, confusion of address and identification fields in packet headers via hashing functions is explored as a technique to help disguise the location of the base station from eavesdroppers. Third, relocation of the base station in the network topology is studied as a means of enhancing resiliency and mitigating the scope of damage. The work can be simulated using the MATLAB environment and results from the various secure techniques can be compared.

References

[1] *A. Mainwaring, J. Polastre, R. Szewczyk D. Culler, J. Anderson, "Wireless Sensor Networks for Habitat Monitoring", First ACM Workshop on Wireless Sensor Networks and Applications (WSNA) 2002, pp. 88-97.*

[2] *F. Martin, B. Mikhak, and B. Silverman, "MetaCricket: A designer's kit for making computational devices," IBM Systems Journal, vol. 39, nos. 3 & 4, 2000.*

[3] *ARGUS Advanced Remote Ground Unattended Sensor Systems, Department of Defense, U.S. Air Force, http://www.globalsecurity.org/intell/systems/arguss.htm.*

[4] *D. Ganesan, R. Govindan, S. Shenker and D. Estrin, "Highly Resilient, Energy Efficient Multipath Routing in Wireless Sensor Networks," Mobile Computing and Communication Review (MC2R) Vol 1., No.2. 2002.*

[5] *A. Perrig, R. Szewczyk, V. Wen, D. Culler, J.D. Tygar, "SPINS: Security Protocols for Sensor Networks," Proceedings of Seventh Annual International Conference on Mobile Computing and Networks MOBICOM 2001, July 2001.*

[6] *Y. Hu, D. Johnson, A. Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks," Fourth IEEE Workshop on Mobile Computing Systems and Applications (WMCSA '02).*

[7] *Y. Hu, A. Perrig, D. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks," Proceedings of the Eighth Annual International Conference on Mobile Computing and Networking (MobiCom 2002).*

[8] *J. Hill, R. Szewczyk, A. Woo, S. Hollar, D. Culler, K. Pister, "System architecture directions for network sensors", ASPLOS 2000.*

[9] *J. Staddon, D. Balfanz, G. Durfee, "Efficient Tracing of Failed Nodes in Sensor Networks", First Workshop on Sensor Networks and Applications, WSNA'02, Atlanta, Georgia, USA.*

[10] *C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", First IEEE International Workshop on Sensor Network Protocols and Applications, May 2003.*

[11] *A. Wood, J. A. Stankovic, "Denial of Service in Sensor Networks," IEEE Computer, 35(10):54-62, October 2002.*

[12] *J. Deng, R. Han and S. Mishra, "The Performance Evaluation of Intrusion-Tolerant Routing in Wireless Sensor Networks", to appear in IEEE 2nd International Workshop on Information Processing in Sensor Networks (IPSN '03), Palo Alto, CA, USA, April, 2003.*

[13] *P. Juang, H. Oki, Y. Wang, M. Martonosi, L. Peh, and D. Rubenstein, "Energy-efficient computing for wildlife tracking: Design tradeoffs and early experiences with zebranet, In ASPLOS 2002, 2002.*

[14] *Y. Hu, A. Perrig, D. Johnson, "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols", Technical Report TR01-384, Department of Computer Science, Rice University, June 2002.*

[15] *J. J. Kong, P. Zerfos, H. Luo, S. Lu, L.X. Zhang, "Providing Robust and Ubiquitous Security Support for Mobile Ad-Hoc Networks", International Conference on Network Protocols (ICNP 2001).*