ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

A Trustworthy & Secure Probability Method for Intrusion Detection and Rouge Node Eviction in a Complex Wireless Sensor Networks

Karla Radhika
M.Tech Student,
Department of CSE,
Medha Engineering College,
Khammam.

M.Supriya Menon, M.Tech
Assistant Professor,
Department of CSE,
Medha Engineering College,
Khammam.

I. Narasimha Rao
Asst Professor & HOD,
Department of CSE,
Medha Engineering College,
Khammam.

Abstract:

A wireless sensor network (WSN) of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on. A heterogeneous wireless sensor networks (HWSNs) consists of two or more types of nodes.

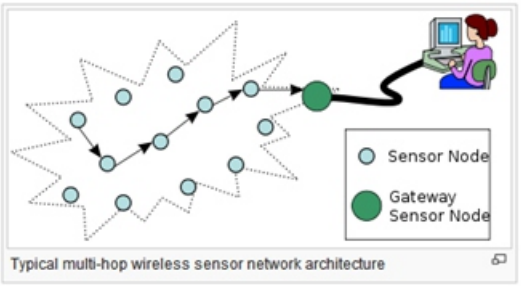
The redundancy management of various wireless sensor networks uses multipath routing to answer user queries in the presence of defective and malicious nodes. The fixed method uses a novel probability model to analyze the best redundancy level in terms of path redundancy (mp) and source redundancy (ms), as well as the best interruption detection settings in terms of the number of voters (m) under which the lifetime of a heterogeneous wireless sensor network is maximized while satisfying the reliability, timeliness and security. The protocol relies on a new multipath constructions paradigm that is defined specifically for heterogeneous WSN. The approach leverages a reasonable increase in the network lifetime and a higher resilience and fault tolerance.

Keywords:

Intrusion detection, multipath routing, fault tolerance, reliability, security, energy conservation.

Introduction:

Wireless sensors networks (WSN) are planned in unattended surroundings in which energy replacement is difficult if not possible. Due to partial income, a WSN should not only assure the application specific QoS requirements such as timeliness, security, and reliability, but also reduce energy consumption to extend the system helpful lifetime.



Typical multi-hop wireless sensor network architecture

The WSN is built of "nodes" – from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. Each such sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting. A sensor node might vary in size from that of a shoebox down to the size of a grain of dust, although functioning "motes" of genuine microscopic dimensions have yet to be created. The cost of sensor nodes is similarly variable, ranging from a few to hundreds of dollars, depending on the complexity of the individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and communications bandwidth.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

The topology of the WSNs can vary from a simple star network to an advanced multi-hop wireless mesh network. The propagation technique between the hops of the network can be routing or flooding.

The main characteristics of a WSN include:

- Power consumption constraints for nodes using batteries or energy harvesting
- Ability to cope with node failures (resilience)
- Mobility of nodes
- Heterogeneity of nodes
- Scalability to large scale of deployment
- Ability to withstand harsh environmental conditions
- Ease of use
- Cross-layer design

Cross-layer is becoming an important studying area for wireless communications. In addition, the traditional layered approach presents three main problems:

- Traditional layered approach cannot share different information among different layers which leads to each layer not having complete information. The traditional layered approach cannot guarantee the optimization of the entire network.
- The traditional layered approach does not have the ability to adapt to the environmental change.
- Because of the interference between the different users, access confliction, fading, and the change of environment in the wireless sensor networks, traditional layered approach for wired networks is not applicable to wireless networks.

Wireless communication and MEMS - the two technologies which have revolutionalized the way we live have also resulted in the development of wireless sensor networks. These comprise of relatively inexpensive sensor nodes capable of collecting, processing, storing and transferring information from one node to another. These nodes are able to autonomously form a network through which sensor readings can be propagated. Since the sensor nodes have some intelligence, data can be processed as it flows through the network. The latter is being done wirelessly these days using networking principles. The flexibility of installation and configuration has greatly improved resulting in a flurry of research activities commencing in the field of sensor networks owing to their ready acceptance in various industries such as security, telecommunications and automobile to name a few. In computing, a wireless intrusion prevention system (WIPS) is a network device that monitors the radio spectrum for the presence of unauthorized access points (intrusion detection), and can automatically take countermeasures (intrusion prevention).

The primary purpose of a WIPS is to prevent unauthorized network access to local area networks and other information assets by wireless devices. These systems are typically implemented as an overlay to an existing Wireless LAN infrastructure, although they may be deployed standalone to enforce no-wireless policies within an organization. Some advanced wireless infrastructure has integrated WIPS capabilities.Large organizations with many employees are particularly vulnerable to security breaches caused by rogue access points. If an employee (trusted entity) in a location brings in an easily available wireless router, the entire network can be exposed to anyone within range of the signals.

A wireless intrusion detection system (WIDS) monitors the radio spectrum for the presence of unauthorized, rogue access points and the use of wireless attack tools. The system monitors the radio spectrum used by wireless LANs, and immediately alerts a systems administrator whenever a rogue access point is detected. Conventionally it is achieved by comparing the MAC address of the participating wireless devices.Rogue devices can spoof MAC address of an authorized network device as their own. New research uses fingerprinting approach to weed out devices with spoofed MAC addresses. The idea is to compare the unique signatures exhibited by the signals emitted by each wireless device against the known signatures of pre-authorized, known wireless devices.In addition to intrusion detection, a WIPS also includes features that prevent against the threat automatically. For automatic prevention, it is required that the WIPS is able to accurately detect and automatically classify a threat.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

The following types of threats can be prevented by a good WIPS:

- Rogue AP – WIPS should understand the difference between Rogue AP and External (neighbor's) AP
- Mis-configured AP
- Client Mis-association
- Unauthorized association
- Man in the Middle Attack
- Ad hoc Networks
- MAC-Spoofing
- Honeypot / Evil Twin Attack
- Denial of Service (DoS) Attack

WIPS configurations consist of three components:

Sensors — These devices contain antennas and radios that scan the wireless spectrum for packets and are installed throughout areas to be protected

Server — The WIPS server centrally analyzes packets captured by sensors

Console — The console provides the primary user interface into the system for administration and reporting

A simple intrusion detection system can be a single computer, connected to a wireless signal processing device, and antennas placed throughout the facility. For huge organizations, a Multi Network Controller provides central control of multiple WIPS servers, while for SOHO or SMB customers, all the functionality of WIPS is available in single box.In a WIPS implementation, users first define the operating wireless policies in the WIPS. The WIPS sensors then analyze the traffic in the air and send this information to WIPS server. The WIPS server correlates the information validates it against the defined policies and classifies if it is a threat. The administrator of the WIPS is then notified of the threat, or, if a policy has been set accordingly, the WIPS takes automatic protection measures.WIPS is configured as either a network implementation or a hosted implementation.

Existing System:

In Existing System, effective redundancy management of a clustered HWSN to prolong its lifetime operation in the presence of unreliable and malicious nodes. We address the tradeoff between energy consumption vs. QoS gain in reliability, timeliness and security with the goal to maximize the lifetime of a clustered HWSN while satisfying application QoS requirements in the context of multipath routing. More specifically, we analyze the optimal amount of redundancy through which data are routed to a remote sink in the presence of unreliable and malicious nodes, so that the query success probability is maximized while maximizing the HWSN lifetime.

Disadvantages:

- It's difficult to detect extensive malicious attacks and insidious attackers
- No security for file

Proposed System:

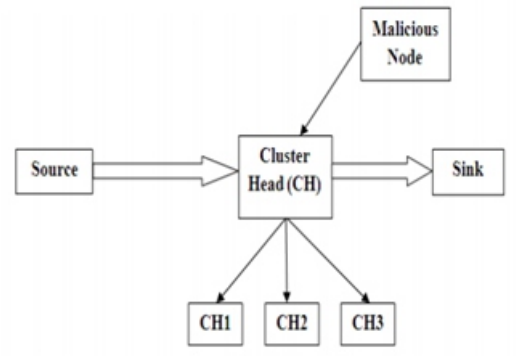
In Proposed System, the optimal communication range and communication mode were derived to maximize the HWSN lifetime. In intra-cluster scheduling and inter-cluster multi-hop routing schemes to maximize the network lifetime. They considered a hierarchal HWSN with CH nodes having larger energy and processing capabilities than normal SNs.The solution is formulated as an optimization problem to balance energy consumption across all nodes with their roles. In either work cited above, no consideration was given to the existence of malicious nodes. A two-tier HWSN with the objective of maximizing network lifetime while fulfilling power management and coverage objectives. They determined the optimal density ratio of the two tier's nodes to maximize the system lifetime.

Advantages:

- Security and Reliability, Easily detect insidious attackers.
- Best intrusion detection in packet dropping, bad mouthing attacks, packet modifier and packet sniffing attack.

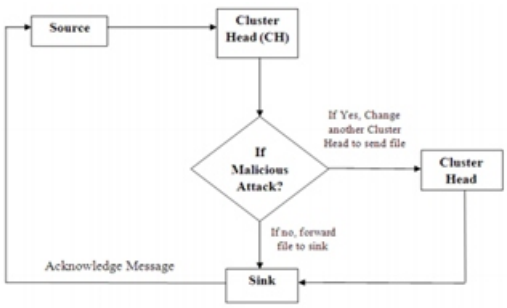
ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Architecture:



In the above Architecture Diagram clearly shows that the cluster head is choose on the basis of voting based algorithm. And each node is taking a part as a monitoring agent and also they can be act as a routing node. The cluster head is changed dynamically to avoid the redundancy in the path and also for to avoid the Hackers to track the path.

Data Flow Diagram:



The sender (Source) can transmit a data to the Receiver (Sink) without any intrusion of other malicious node i.e. Hacker System. To avoid this problem the sender uses a Multi path routing to transfer the data securely with the help of the transferring and monitoring agent called Cluster Head. In the HWSN the each system is considered as the node. The Cluster node is choose by a voting based Algorithm.

MODULES:

1.Multi – Path Routing

2.Intrusion Tolerance

3.Energy Efficient

4.Simulation Process

Modules Description:

Multi – Path Routing

In this module, Multipath routing is considered an effective mechanism for fault and intrusion tolerance to improve data delivery in WSNs. The basic idea is that the probability of atleast one path reaching the sink node or base station increases as we have more paths doing data delivery. While most prior research focused on using multipath routing to improve reliability, some attention has been paid to using multipath routing to tolerate insider attacks. These studies, however, largely ignored the tradeoff between QoS gain vs. energy consumption which can adversely shorten the system lifetime.

Intrusion Tolerance

In this Modules, intrusion tolerance through multipath routing, there are two major problems to solve:
(1) How many paths to use and
(2) What paths to use.
To the best of our knowledge, we are the first to address the “how many paths to use” problem. For the “what paths to use” problem, our approach is distinct from existing work in that we do not consider specific routing protocols.

Energy Efficient

In this module, there are two approaches by which energy efficient IDS can be implemented in WSNs. One approach especially applicable to flat WSNs is for an intermediate node to feedback maliciousness and energy status of its neighbor nodes to the sender node (e.g., the source or sink node) who can then utilize the knowledge to route packets to avoid nodes with unacceptable maliciousness or energy status. Another approach which we adopt in this paper is to use local host-based IDS for energy conservation.

Simulation Process:

In this module, the cost of executing the dynamic redundancy management algorithm described above, including periodic clustering, periodic intrusion detection, and query processing through multipath routing, in terms of energy consumption.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Conclusion:

In HSWN, performance of a tradeoff analysis of energy consumption vs. QoS gain in reliability, timeliness, and security for redundancy management of clustered heterogeneous wireless sensor networks utilizing multipath routing to answer user queries. We developed a novel probability model to analyze the best redundancy level in terms of path redundancy (mp) and source redundancy (ms), as well as the best intrusion detection settings in terms of the number of voters (m) and the intrusion invocation interval (TDS) under which the lifetime of a heterogeneous wireless sensor network is maximized while satisfying the reliability, timeliness and security requirements of query processing applications in the presence of unreliable wireless communication and malicious nodes.

Finally, we applied our analysis results to the design of a dynamic redundancy management algorithm to identify and apply the best design parameter settings at runtime in response to environment changes to prolong the system lifetime.

REFERENCES:

[1] Hamid Al-Hamadi and Ing-Ray Chen, "Redundancy Management of Multipath Routing for Intrusion Tolerance in Heterogeneous Wireless Sensor Networks," IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT, VOL. 10, NO. 2, JUNE 2013.

[2] O. Younis and S. Fahmy, "HEED: a hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks," IEEE Trans. Mobile Comput., vol. 3, no. 4, pp. 366–379, 2004.

[3] E. Felemban, L. et al, "MMSPEED: multipath multi-SPEED protocol for QoS guarantee of reliability and timeliness in wireless sensor networks," IEEE Trans. Mobile Comput., vol. 5, no. 6, pp.738–754.

[4] I. R. Chen, et.al, "Adaptive fault-tolerant QoS control algorithms for maximizing system lifetime of query-based wireless sensor networks," IEEE Trans. Dependable Secure Computing, vol. 8, no. 2, pp. 161–176, 2011.

[5] M. Yarvis, N. Kushalnagar, H. Singh, A. Rangarajan, Y. Liu, and S.Singh, "Exploiting heterogeneity in sensor networks," in Proc. 2005 IEEE Conf. Computer Commun., vol. 2, pp. 878–890

[6] H. M. Ammari and S. K. Das, "Promoting heterogeneity, mobility, and energy-aware Voronoi diagram in wireless sensor networks," IEEE Trans. Parallel Distrib. Syst., vol. 19, no. 7, pp. 995–1008, 2008.

[7] X. Du and F. Lin, "Improving routing in sensor networks with heterogeneous sensor nodes," in Proc. 2005 IEEE Veh. Technol. Conf., pp. 2528–2532.

[8] S. Bo, L. Osborne, X. Yang, and S. Guizani, "Intrusion detection techniques in mobile ad hoc and wireless sensor networks," IEEE Wireless Commun. Mag., vol. 14, no. 5, pp. 560–563, 2007

[9] I. Krontiris, T. Dimitriou, and F. C. Freiling, "Towards intrusion detection in wireless sensor networks," in Proc. 2007 European Wireless Conf.

[10] J. H. Cho, I. R. Chen, and P. G. Feng, "Effect of intrusion detection on reliability of mission-oriented mobile group systems in mobile ad hoc networks," IEEE Trans. Reliab., vol. 59, no. 1, pp. 231–241, 2010.

[11] A. P. R. da Silva, M. H. T. Martins, B. P. S. Rocha, A. A. F. Loureiro, L.B. Ruiz, and H. C. Wong,

"Decentralized intrusion detection in wireless sensor networks," in Proc. 2005 ACM Workshop Quality Service Security Wireless Mobile Net.

[12] Y. Zhou, Y. Fang, et.al., "Securing wireless sensor networks: a survey," IEEE Commun. Surveys & Tutorials,vol. 10, no. 3, pp. 6–28, 2008.

[13] Y. Yang, C. Zhong, Y. Sun, and J. Yang, "Network coding based reliable disjoint and braided multipath routing for sensor networks," J. Netw. Comput. Appl., vol. 33, no. 4, pp. 422–432, 2010.

[14] J. Deng, et. al, "INSENS: intrusion-tolerant routing for wireless sensor networks," Computer Commun., vol. 29, no. 2, pp. 216–230, 2006