JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Challenges in Combining WSNs and Mobile Agents

1 Anurag Pathak

J.P Institute of Engineering and Technology, Meerut

[2]Ayan Rajput

Assistant Professor

Department of Computer Science & Engineering

J.P Institute of Engineering and Technology, Meerut

Abstract:-

Integrating Wireless Sensor Networks (WSNs) with mobile agents has emerged as a promising solution for enhancing the efficiency and scalability of data collection and processing in dynamic environments. However, this integration is not without its challenges.
This paper identifies and discusses the key challenges in combining WSNs and mobile agents, including issues related to network connectivity, resource management, security, and Algorithm Design.Further more, the paper proposes potential solutions and best practices to address these challenges and improve the performance of WSNs with mobile agents.
By addressing these challenges, researchers and practitioners can unlock the full potential of combining WSNs and mobile agents for various applications, such as environmental monitoring, smart cities, and healthcare systems.

Keywords :- Wireless Sensor Networks (WSNs), Mobile Agents,**Energy Consumption**, **Communication Overhead,Mobility Management,Security Concerns**, **Fault Tolerance and Reliability**.

1 Introduction :-

The integration of Wireless Sensor Networks (WSNs) with mobile agents presents a multitude of challenges that need to be addressed for successful implementation. This research paper aims to explore the complexities associated with combining these two technologies and highlight the potential obstacles that researchers and developers may encounter.

By investigating the synergy between WSNs and mobile agents, we can gain valuable insights into optimizing their collaboration for enhanced data collection, processing, and dissemination in dynamic environments.

Through a comprehensive review of existing literature and case studies, this paper will shed light on key challenges such as network scalability, energy efficiency, security, routing protocols, and task allocation strategies.

Ultimately, this research will contribute to advancing the field of IoT and intelligent systems by offering practical solutions to overcome the barriers in integrating WSNs with mobile agents.

2 Mobile Agents :-

A mobile agent is a self-contained programme that can move from one host to another in a network and interact with resources and other agents [2].

Because the state of the running programme is preserved and subsequently transferred to the new host, there is little possibility of data loss during this procedure.

It enables the programme to resume execution where it left off prior to migration. The most major advantage of mobile agents is the ability to relocate complicated processing operations to locations where massive amounts of data must be processed. In Other Words is known as transportable agents. Mobile Agents with a Static Migration Path: They have a pre-defined migration path. Roamer and other mobile agents with an unknown path have dynamic migration paths.[1]

2.1 Features of Mobile Agents :-

According to Nawana Its purpose is to look into agent typologies. The study of different sorts of entities is known as typology. Existing software agents can be classified along numerous dimensions. To begin; agents can be categorized according to their mobility.

They can also be classified as deliberate or reactive. Finally, agents can be defined based on a set of ideal and primary characteristics that they should possess. At BT Labs, we've narrowed it down to three: autonomy, learning, and cooperation. [2]

Nwana describes ongoing research in seven areas after defining this typology. The mobile agents are intelligent, social, and learnable, and their mobility is their most important quality.

They are self-contained, self-driven, and do not require a communication node to function. Even if the user is removed from the network, they can continue to operate effectively. [3]

Intelligence:- Mobile Agents have the cap potential to investigate and look for data in their vicinity. Because they have some vicinity expertise, they may be called smart agents.

Mobility :- They can go from one node to another and perform activities while doing so.

Communicative :- Mobile agents use a communication language to handle inter-agent communication.[4]

2.1 Network management

Mobile agent technology provides a solution to the flexible management of network systems. Mobile agents can locally observe and control equipment at each node by migrating among nodes. Mobile agent-based network management has several advantages in comparison with traditional approaches, such as the client/server one.[9]

1.As code is very often smaller than the data it processes, the transmission of mobile agents to sources of data creates less traffic than transferring the data itself. Deploying a mobile agent close to the network nodes that we want to monitor and control prevents delays caused by network congestion.

2. Since a mobile agent is locally executed on the node it is visiting, it can easily access the functions of devices on this node.

3.The dynamic deployment and con of new or existing functionalities into a network system are extremely important tasks, especially as they potentially allow outdated systems to be updated in an efficient manner.

4.Network management systems must often handle networks that may have various malfunctions and disconnections and whose exact topology may not be known. Since mobile agents are autonomous entities, they may be able to detect proper destinations or routings on such networks.[9]

Adopting mobile agent technology eliminates the need for administrators to constantly monitor many network management activities, e.g., the installation and upgrading of software and periodic network auditing. There have been several attempts to apply this technology to network management tasks. Karmouch presented typical mobile agent approaches to network management [10].

Satoh proposed a framework for building and operating agent itineraries for network management systems [11,12] and constructed domain-specific languages for describing agent migration for network management [13].

3 Wireless Sensor Networks (WSNs)

1. WSNs are autonomous systems consisting of spatially-distributed sensing devices called sensor nodes.

2.Sensor nodes gather data from the surrounding environment and transmit it wirelessly to the base station or gateway.

3.Sensor nodes typically contain a microcontroller, transceiver, power supply, and sensors to measure physical quantities such as temperature, humidity, and light intensity.

3.1 Applications and Advantages of WSNs:

1.Environmental Monitoring: WSNs enable real-time monitoring of environmental factors, such as air quality, water quality, and soil conditions.

2.Healthcare: WSNs assist in remote patient monitoring, fall detection, and tracking vital signs.

3.Industrial Automation: WSNs facilitate predictive maintenance, energy management, and monitoring of manufacturing processes.

4.Precision Agriculture: WSNs enhance crop yield by monitoring soil moisture levels, detecting pests, and automating irrigation systems.

5.Advantages of WSNs include cost-effectiveness, scalability, ease of deployment, and flexibility in various applications.

4 Mobile Agents and Wireless Networks

The traditional protocols of the WSNs have used the computer-to-computer communication as Remote Procedure Calling (RPC). It enables a computer to call procedures in another computer across the network [5].

Each message transmitted by the network either request or acknowledge is represented as a procedure's task. A request includes data that are the procedure's argument. The response includes data that represents its results. On the other side, mobile agents have been used as an alternative method that belongs to computer- to-computer communication methodology.

It is a remote procedure that has used Remote Programming (RP) to enable a computer to call procedures in another computer and supply the procedure to be performed [6]. The messages transported in the network contain a procedure only, while the data is static.

However, mobile agents are programs that can move from one computer to another in a network or at times to any host of their choice making them autonomous. Using the mobile agents for WSNs can improve their performance and save the data. But, on the other side, moving the mobile agents around the network can face some threats.

Thus, there are four known threat MA, namely: The Agent- to-Host, Agent-to-Agent, Host-to-Agent, Other-to-Agent Host attacks are the kinds of security attacks that are possible in a Mobile Agent System [7].

5 Challenges in Combining WSNs and Mobile Agents:

Methodology :-

Combining Wireless Sensor Networks (WSNs) and Mobile Agents (MAs) involves several technical and practical challenges. Addressing these challenges often requires a mix of theoretical formulas, simulation models, and real-world data. Here's a closer look at some of the specific challenges and how they might be approached with formulas and real data:

1. Energy Consumption

Challenge: Mobile agents can increase energy consumption in WSNs due to their movement and data processing requirements.

Formulas:

Energy Consumption for Data Transmission:-

Etx=Etx_per_bit×d^2×L

where Etx is the energy consumed in transmission, (Etx_per_bitis the energy consumed per bit, d is the distance to the receiver, and L is the number of bits transmitted.

Energy Consumption for Mobile Agents:-

Eagent = Emove x M + Ecomp x T

where (Eagent) is the total energy consumed by the mobile agent, (Emove) is the energy consumed per unit distance traveled, (M) is the distance traveled, (Ecomp) is the energy consumed per computation task, and (T) is the number of tasks performed.

Real Data:- Energy consumption data for specific sensor nodes and mobile agents can be gathered from experiments or simulation studies. For instance, data might be collected from actual sensor nodes in a test environment or from simulations that model realistic network conditions.

2. Communication Overhead

Challenge:- Mobile agents introduce additional communication overhead, which can lead to network congestion.

Formulas:
Communication Overhead:

Ocomm = Nmsg x (H + L)/T

where Ocomm is the communication overhead, Nmsg is the number of messages exchanged, (H) is the header size, (L) is the payload size, and (T) is the time period.

Real Data: Communication overhead can be measured in real deployments by capturing network traffic and analyzing the number of messages, header sizes, and payloads. Simulation tools can also provide insights into how overhead changes with different agent behaviors and network configurations.

3. Mobility Management

Challenge: Efficiently managing the movement of mobile agents across the network.

Formulas:

Optimal Path Calculation:

$$d_{path} = \sum_{i=1}^{N-1} \sqrt{(x_i - x_{i+1})^2 + (y_i - y_{i+1})^2}$$

where d_{path} is the total distance of the path, $((x_i, y_i))$ are the coordinates of the waypoints, and (N) is the number of waypoints.

Real Data: Real-world mobility patterns can be studied using GPS data from mobile agents or nodes in experimental setups. This data helps in refining algorithms for optimal path planning and mobility management.

4. Security Concerns

Challenge: Securing the communication and behavior of mobile agents within WSNs.

Formulas:

Energy Cost for Security Measures:

$$[E_{sec} = E_{enc} \times L + E_{auth} \times N_{auth}]$$

where (Esec) is the total energy for security, (Eenc) is the energy required for encryption per bit, (L) is the data length, (Eauth) is the energy for authentication, and (Nauth) is the number of authentication operations.

Real Data: Security-related energy costs and the effectiveness of different security protocols can be measured through experiments and simulations. Real data from network deployments can help in understanding the impact of various security measures on overall system performance.

5.Fault Tolerance and Reliability

Challenge: Ensuring the system remains robust despite failures or unreliable nodes.

Formulas:

$$R_{agent} = 1 - \prod_{i=1}^{N} (1 - p_i)]$$

where (Ragent) is the reliability of mobile agents, and (pi) is the probability of failure for each agent.

Real Data: Fault tolerance and reliability can be evaluated using data from deployments or simulations where nodes or agents fail. This data helps in understanding the impact of failures and in designing more resilient systems.

6 Future Work And Facts :-

6.1 Proposed Security System

The proposed system has suggested the use of mobile agents for the WSNs security. The suggested system uses mobile agents for collecting and analyzing the data in the wireless environment. It uses different types of agents to detect the attacks. They are: collector agent, misuse detection agent, attack detection agent, and alert agent.

1- Collector Agent

The collector agent collects the data from the wireless environment. Then, it stores the data in the file.

2- Misuse Detection Agent

The misuse detection agent is used to analyze the data acquired for having attacks in the network, and reports it to the alert agent.

3-Attacks Detection Agent

The attacks detection agent is used to detect the attacks facing the WSN.

4- Alert Agent

The alert agent is used to alert the system if any attack occurs in the network. However, the operation of the proposed system can be described as: The collector agent is used to acquire the data from the wireless environment and store it as a file. This file is used by the misuse detection agent. It analyzes the data by matching it to its reference. If any attack appears, it reports it to alert agents and updates the database about the attack.

On the other hand, the proposed security algorithm is concerned with two main types of attacks. They are: Clone and sink hole attacks. Each of these attacks is handled by a separate module.

6.2 Proposed Mobile Agents Based Clone Attack Detection (MACAD) Algorithm

The proposed Mobile Agents Based Clone Attack Detection (MACAD) Algorithm can be explained in the following steps:

1- Identify the location of each node (for ex: node A) in the network and also identify its location and signature for a group of its neighbor nodes (N).

2- Mobile agent gets the signed location claim of each node and stores it in its defined cell in the node's information matrix. This matrix is constructed through the mobile agent routing algorithm.

3- At run-time, each node must be verified by its signature and plausibility of location by each node in its neighboring group (N).[8]

4- If more than one entry for a signed location claim appears in a single cell of an information matrix of one node. This is achieved only when a mobile agent has a different latest location claim for the same node i. In this case, mobile agent broadcasts the two conflicting claims as evidence to the network's nodes in order to prevent this repetition.

5- The proposed system broadcasts the event to every node in the entire network. Therefore, a real node will not replay for the inaccurate information from malicious people.

6- The proposed system has used the mobile agents to execute steps 4 and 5. [8]

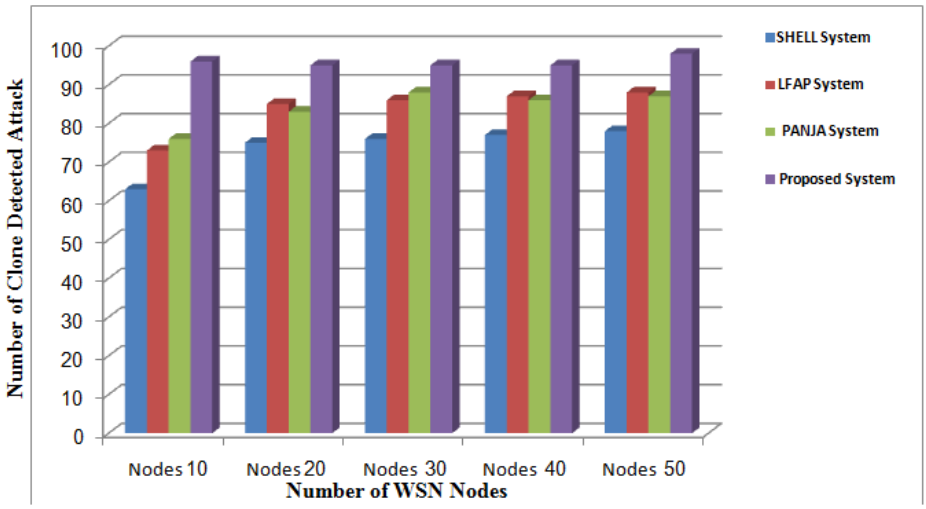

Fig. (1): Comparison between the number of Clone Detected Attacks by the proposed system with mobile agents and the three traditional security systems at deployed nodes. [8]

Conclusion:-

The integration of WSNs with mobile agents offers significant potential for enhanced network capabilities and flexibility, but it also requires addressing several complex challenges.

Balancing energy efficiency, managing communication overhead, optimizing mobility, securing the network, and ensuring reliability are critical to achieving a successful integration.

Effective solutions often involve a combination of theoretical models, empirical data, and practical experimentation. By leveraging advanced algorithms, energy-efficient designs, and robust security measures, the combined use of WSNs and mobile agents can be optimized to deliver powerful and reliable systems for various applications.

Ongoing research and development in this field are essential to overcoming the existing challenges and realizing the full potential of these technologies.

References :-

1. Yojana,Umesh Kumar Assistant Professor, Dept. of Computer Engineering, Ymca Ust, Mobile Agent : A Review International Journal of Management, Technology And Engineering 2019.

2."Proceedings of International Conference on Internet Computing and Information Communications", Springer Science and Business Media LLC, 2014.

3.Mohit Mittal Assistant Professor, MOBILE AGENT International Journal of Engineering Research & Technology (IJERT)2012.

4. Ayan Rajput and Sandeep Rana/ Elixir Comp. Engg. 167 (2022) 56276-56279.

5. B. M. Thippeswamy, (2015), "STEAR: Secure Trust-Aware Energy-Efficient Adaptive Routing in Wireless Sensor Network",Journal of Advances in Computer Networks, Vol. 3, No. 2, pp.146-149.

6. G. Zhan, W. Shi, and J. Deng, (2012), “Design and implementation of TARF: A Trust Aware Routing Framework For WSNs,” IEEE Transactions on Dependable and Secure Computing, Vol. 9, No. 2, pp. 184-197, March/April 2012

7. D. D. Geetha, N. Nalini, (March 2014), " Trust based Neighbor Identification in Wireless Sensor Networks using Agents ",International Journal of Emerging Technology and Advanced Engineering , Volume 4, Issue 3 , pp.178-187.

8. IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 4, Ver. I (Jul.-Aug. 2016), PP 77-82 www.iosrjournals.org.

9. Mobile Agents. Ichiro Satoh.

10. V. A. Pham, A Karmouch, Mobile Software Agents: An Overview, IEEE Communications Magazine, vol. 36 no. 7, pp.26-37, July 1998.

11.I. Satoh, Building Reusable Mobile Agents for Network Management, IEEE Transactions on Systems, Man and Cybernetics, vol.33, no. 3, part-C, pp.350-357, August 2003.

12.I. Satoh, Selection of Mobile Agents, Proceedings of 24th IEEE International Conference on Distributed Computing Systems (ICDCSb2004), pp.484-493, IEEE Computer Society, March 2004.

13. I. Satoh, Building and Selecting Mobile Agents for Network Management, Journal of Network and Systems Management, vol.14, no.1, pp.147-169, Springer, 2006.