ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 2, February 2014

PROBABILITY OF ROUTING PACKET IN HETEROGENEOUS WIRELESS SENSOR NETWORK

S.ABIRAMI[1], B.VIJAYANIRMALA[2], N.DEEPA[3]

Assistant Professors, Department of Computer Science and Engineering, R.V.S Educational Trust's Group of Institutions, R.V.S School of Engineering and Technology, Dindigul, TamilNadu, India[1,2,3]

Abstract: 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 cruel 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*) and the intrusion invocation interval (T_{IDS}) under which the lifetime of a heterogeneous wireless sensor network is maximized while satisfying the reliability, timeliness and security. In propose we plan to explore more extensive malicious attacks in addition to packet reducing and bad mouthing attacks, each with different implications to energy, security and reliability, and investigate intrusion detection and multipath routing based acceptance protocols to react to these attacks.

I. INTRODUCTION

Many wireless sensor networks (WSNs) are deployed in an unattended environment in which energy replenishment is difficult if not impossible. Due to limited resources, a WSN must not only satisfy the application specific QoS requirements such as reliability, timeliness and security, but also minimize energy consumption to prolong the system useful lifetime. The tradeoff between energy consumption vs reliability gain with the goal to maximize the WSN system lifetime has been well explored in the literature.

1.1 MOBILE COMMUNICATION

Mobile communications today has heterogeneous wireless networks providing varying coverage and QoS. Various communication services are available. The infrastructure enables mobile devices to run applications with diverse bandwidth and network connectivity requirements, such as distributed speech recognition, video streaming, gaming etc. To satisfy the bandwidth and QoS constraints of the applications, the mobile devices need to allow seamless switching among various wireless network interfaces. Additionally, the high communication and computation cost of applications is a burden on the battery life of portable devices. We implemented the policy on HP's IPAQ portable device that is communicating with HP's Hot Spot server via Bluetooth and 802.11b. The applications we tested range From MPEG video to email. Our results show both large savings in power when using a single WNIC, as well as seamless switching with concurrent power savings among WNICs.

1.2 REDUNDANCY WSN

A WSN is a special type of Ad hoc networks containing several sensor nodes which are able to collect data and to transmit it using a multi-jump routing protocol to the collection point, called Sink node each node gets his energy from an individual battery that consumption due to the communication and data processing must be optimized. The important density of sensor nodes implies the existence of redundant nodes. Generally, the breakdowns in a WSN can be caused by the mobility or the exhaustion of the nodes energy. These breakdowns must be detected and solved in an acceptable time without affecting quality of service.

This centralization of diagnosis and reconfiguration operations in only one module (Sink in general) presents major disadvantages:

- Overload of the monitoring module by control treatments.
- Overload of all the nodes in network by the control and reconfiguration messages, which increases considerably energy consumption especially in the case of large scales networks. So WSN life time is reduced.
- The failure detection can be delayed because Transmission times.
- The failure of the monitoring module paralyzes the operation of the entire network.

1.3 ABOUT THE PROJECT

Many wireless sensor networks (WSNs) are deployed in an unattended environment in which energy replenishment is difficult if not impossible. 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 at least 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. The research problem we are addressing in this

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 2, February 2014

paper is 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.

II. SYSTEM ANALYSIS

2.1 EXISTING SYSTEM

The prior work performed 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 (T_{IDS}) 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. But it cannot perform extensive malicious attacks and insidious attackers.

Disadvantages:

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

2.2 PROPOSED SYSTEM

In proposed system, we plan to explore more extensive malicious attacks in addition to packet dropping and bad mouthing attacks, each with different implications to energy, security and reliability, and investigate intrusion detection and multipath routing based tolerance protocols to react to these attacks. Another direction is to consider smart and insidious attackers which can perform more targeted attacks, capture certain strategic nodes with higher probability, alternate between benign and malicious behavior and collude with other attackers to avoid intrusion detection. Lastly, we plan to investigate the use of trust/reputation management to strengthen intrusion detection through "weighted voting" leveraging knowledge of trust/reputation of neighbor nodes, as well as to tackle the "what paths to use" problem in multipath routing decision making for intrusion tolerance in WSNs.

Advantages

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

III. SYSTEM DESIGN

3.1ROUTING TRANSACTION

File transfer is a generic term for the act of transmitting files from source to destination or sender to receiver or client to server over a computer network like the Internet. There are numerous ways to transfer files over a network. Computers which provide a file transfer service are often called file servers. Depending on the client's perspective the data transfer is called uploading or downloading.

3.2 MULTIPATH ROUTING

The 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 at least 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.

In the context of secure multipath routing for intrusion tolerance, provides an excellent survey in this topic. The authors considered a multipath routing protocol to tolerate black hole and selective forwarding attacks. The basic idea is to use overhearing to avoid sending packets to malicious nodes. Our work also uses multipath routing to tolerate intrusion. However, we specifically consider energy being consumed for intrusion detection, and both CHs and SNs can be compromised for lifetime maximization.

3.3 INTRUSION DETECTION SYSTEM

An intrusion detection system (IDS) has the goal to detect and remove malicious nodes. A voting-based distributed intrusion detection algorithm is applied to remove malicious nodes from the HWSN. To remove malicious nodes from the system, a voting based distributed IDS is applied periodically in every T_{IDS} time interval. A CH is being assessed by its neighbour CHs, and a SN is being assessed by its neighbour SNs. In each interval, *m* neighbour nodes (at the CH or SN level) around a target node will be chosen randomly as voters and each cast their votes based on their host IDS results to collectively decide if the target node is still a good node.

3.4 ENERGY CONVSERVATION CONSUMPTION

In general 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 neighbour 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, coupled with voting to cope with node collusion for implementing IDS function. Energy efficiency is achieved by applying the optimal detection interval to perform IDS functions. Our solution considers the optimal IDS detection interval that can best balance intrusion accuracy vs. energy consumption due to intrusion detection activities, so as to maximize the system lifetime.

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

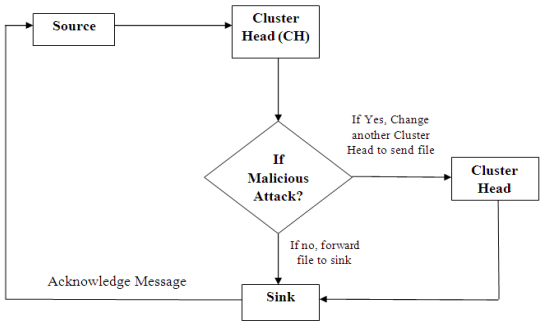
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 2, February 2014

3.5 PERFORMANCE EVALUATION

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 (T_{IDS}) 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.

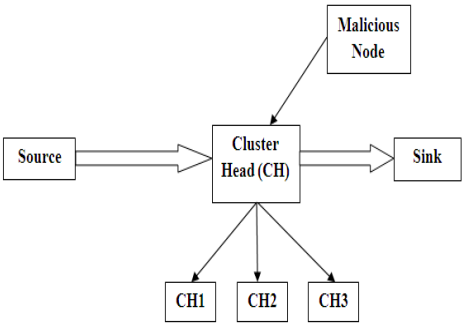
IV. SYSTEM ARCHITECTURE

4.1 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.

4.2 ARCHITECTURE DIAGRAM



In 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.

V. SOFTWARE DESCRIPTIONS

5.1 FRONT END Servlets in J2EE

The Sun Microsystems's java server pages technology allows you to rapidly develop and easily maintain rich, dynamic web pages. As a part of java family JSP enables development of web based applications that are platform independent. The window applications build using Servlet technology works with a wide variety of web servers, application servers, browsers and development tools. The logic that generates the content is encapsulated in tags and JavaBeans components and tied together in script lets, all of which are executed on the server side. If the core logic is encapsulated in tags and Beans then other individuals, such as web masters and page designers, can edit and work with packages without affecting the content. Thus the Servlet technology separates the user interface from the content generation.

Features

- Servlet technology follows the write once run anywhere rule which is the basic of the java language
- Networking uses pure java and takes the advantage of its object oriented nature.
- J2EE Frame work uses a combination of in-built functions and drag & drop to create a form easily.
- The J2EE packages have the components like EJB, JavaBeans which are reusable. This gives the code reusability capabilities.

Applications made using JAVA technology are easier to maintain

5.2 BACK END MySql

MySQL was developed by a consulting firm in Sweden called TcX. They were in need of a database system that was extremely fast and flexible. Unfortunately they could not find anything on the market that could do what they wanted. So, they created MySQL, which is loosely based on another database management system called SQL. The product they created was fast, reliable, and extremely flexible. It is used in many places throughout the world. Lately, however, it has begun to permeate the business world as a reliable and fast database system MySQL is often confused with SQL, the structured query language developed by IBM. It is not a form of this language but a database system that uses SQL to manipulate, create, and show data. MySQL is a program that manages databases, much like Microsoft's Excel manages spreadsheets. SQL is a programming language that is used by MySQL to accomplish tasks within a database, just as Excel uses VBA (Visual Basic for Applications) to handle tasks with spreadsheets and workbooks.

VI. CONCLUSION AND FUTURE WORKS

6.1CONCLUSION

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.

6.2 FUTURE WORK

For future work, plan to explore more extensive malicious attacks in addition to packet dropping and bad mouthing attacks, each with different implications to energy, security and reliability, and investigate intrusion detection and multipath routing based tolerance protocols to react to these attacks. Another direction is to consider smart and insidious attackers which can perform more targeted attacks, capture certain strategic nodes with higher probability, alternate between benign and malicious behaviour and collude with other attackers to avoid intrusion detection.

REFERENCES

[1] E.Felemban, L.Chang-Gun and E.Ekici,"MMSPEED: multipath Multispeed protocol for QoS guarantee of reliability and. Timeliness in wireless sensor networks," IEEE Trans. Mobile Computers., vol. 5, no. 6, 2006.

[2] I.R.Chen,A.P.Speer and M.Eltoweissy, "Adaptive Fault-Tolerant QoS Control Algorithms for Maximizing System Lifetime of Query Based Wireless Sensor Networks," IEEE Trans.on Dependable and Secure Computing, vol. 8, 2011.

[3] 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, 2008.

[4] S.Bo, L.Osborne, X.Yang and S. Guizani, "Intrusion detection techniques in mobile ad hoc and wireless sensor networks," IEEE Wireless Commun., vol. 14, 2007.

[5] I.Krontiris, T.Dimitriou and F.C. Freiling,"Towards intrusion detection in wireless sensor networks," 13th European Wireless Conference, Paris, France, 2007.

[6] 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. Rel., vol. 59, 2010.