ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Routing Attack Discovery in WSN

J. Sabatini[1], Mrs. K. Vanitha, M.E., (Ph.D) [2]

II ME (CSE), Dept. of CSE, Al-Ameen Engineering College, Erode, Tamilnadu, India[1]

Assistant Professor, Dept. of CSE, Al-Ameen Engineering College, Erode, Tamilnadu, India[2]

Abstract: Sensor devices are small devices used to capture information from environment. Capture, store and transmission are the main operations of sensor devices. Temperature, humidity, density of carbon dioxide and pressure details are captured by sensor devices. Battery power is the main limitation of sensor devices. The intrusion detection system identifies the legitimate and attackers in the network area. The intrusion detection system is designed in two categories. In the first model a system component is used for monitoring the security of a WSN and diagnosing compromised/vulnerable. Second model is the monitoring or surveillance system for detecting a malicious intruder that invades the network domain.

Denial of communication is raised at the routing or medium access control levels. Resource depletion attacks are initiated at the routing protocol layer to permanently disable networks by consuming the battery power. Vampire attacks disrupt the network resources at the routing protocol levels. Stateful (Link state and distance vector) protocols and stateless (Dynamic Source Routing) protocols are verified with attacks. Clean-slate secure sensor network routing protocol is modified to control vampire attacks with resource usage analysis.

Clean-slate secure sensor network routing protocol is improved with optimal boundary estimation model. Topology estimation and packet forwarding prediction is integrated. Transmission coverage factors are integrated with the detection scheme. Energy levels and forwarding packet count information are analyzed to improve the network lifetime.

I. INTRODUCTION

A wireless sensor network (WSN) is a wireless network consisting of spatially distributed autonomous devices using sensors to cooperatively monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants, at different locations. The development of wireless sensor networks was originally motivated by military applications such as battlefield surveillance. However, wireless sensor networks are now used in many civilian application areas, including environment and habitat monitoring, healthcare applications, home automation, and traffic control. In addition to one or more sensors, each node in a sensor network is typically equipped with a radio transceiver or other wireless communications device, a small microcontroller, and an energy source, usually a battery. The envisaged size of a single sensor node can vary from shoebox-sized nodes down to devices the size of 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 hundreds of dollars to a few cents, depending on the size of the sensor network and the complexity required of individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and bandwidth. A sensor network normally constitutes a wireless ad-hoc network, meaning that each sensor supports a multi-hop routing algorithm. In computer science and telecommunications, wireless sensor networks are an active research area with numerous workshops and conferences arranged each year.

The applications for WSNs are many and varied, but typically involve some kind of monitoring, tracking, and controlling. Specific applications for WSNs include habitat monitoring, object tracking, nuclear reactor control, fire detection, and traffic monitoring. In a typical application, a WSN is scattered in a region where it is meant to collect data through its sensor nodes.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Area monitoring is a common application of WSNs. In area monitoring, the WSN is deployed over a region where some phenomenon is to be monitored. As an example, a large quantity of sensor nodes could be deployed over a battlefield to detect enemy intrusion instead of using landmines. When the sensors detect the event being monitored, the event needs to be reported to one of the base stations, which can take appropriate action. Depending on the exact application, different objective functions will require different data-propagation strategies, depending on things such as need for *real-time* response, *redundancy* of the data, need for *security*, etc. A number of WSN deployments have been done in the past in the context of environmental monitoring. Many of these have been short lived, often due to the prototypical nature of the projects. A more long-lived deployment is monitoring the state of permafrost in the swiss alps.

II. RELATED WORK

We do not imply that power draining itself is novel, but rather that these attacks have not been rigorously defined, evaluated, or mitigated at the routing layer. A very early mention of power exhaustion as "sleep deprivation torture." As per the name, the proposed attack prevents nodes from entering a low-power sleep cycle, and thus deplete their batteries faster. Newer research on "denial-of-sleep" only considers attacks at the MAC layer [9]. Additional work mentions resource exhaustion at the MAC and transport layers [6] but only offers rate limiting and elimination of insider adversaries as potential solutions. Malicious cycles have been briefly mentioned [5], but no effective defenses are discussed other than increasing efficiency of the underlying MAC and routing protocols or switching away from source routing. Such attacks can be defeated or attenuated by putting greater burden on the connecting entity. There is also significant past literature on attacks and defenses against quality of service (QoS) degradation, or RoQ attacks, that produce long-term degradation in network performance [1], [2], [4]. The focus of this work is on the transport layer rather than routing protocols, so these defenses are not applicable. Moreover, since Vampires do not drop packets, the quality of the malicious path itself may remain high. Other work on denial of service in ad hoc wireless networks has primarily dealt with adversaries who prevent route setup, disrupt communication, or preferentially establish routes through themselves to drop, manipulate, or monitor packets [10]. The effect of denial or degradation of service on battery life and other finite node resources has not generally been a security consideration, making our work tangential to the research mentioned above. Protocols that define security in terms of path discovery success, ensuring that only valid network paths are found, cannot protect against Vampire attacks, since Vampires do not use or return illegal routes or prevent communication in the short term.

Current work in minimal-energy routing, which aims to increase the lifetime of power-constrained networks by using less energy to transmit and receive packets is likewise orthogonal: these protocols focus on cooperative nodes and not malicious scenarios. Additional on power-conserving MAC, upper layer protocols, and cross-layer cooperation [11]. However, Vampires will increase energy usage even in minimal-energy routing scenarios and when power conserving MAC protocols are used; these attacks cannot be prevented at the MAC layer or through cross-layer feedback. Deng et al. discuss path-based DoS attacks and defenses in [8], including using one-way hash chains to limit the number of packets sent by a given node, limiting the rate at which nodes can transmit packets. While this strategy may protect against traditional DoS, where the malefactor overwhelms honest nodes with large amounts of data, it does not protect against "intelligent" adversaries who use a small number of packets or do not originate packets at all. Another attack that can be thought of as path based is the wormhole attack, first introduced. It allows two nonneighboring malicious nodes with either a physical or virtual private connection to emulate a neighbor relationship, even in secure routing systems [3]. These links are not made visible to other network members, but can be used by the colluding nodes to privately exchange messages. Similar tricks can be played using directional antennas. These attacks deny service by disrupting route discovery, returning routes that traverse the wormhole, and may have artificially low associated cost metrics. While the authors propose a defense against wormhole and directional antenna attacks, their solution comes at a high cost and is not always applicable. First, one flavor of Packet Leashes relies on tightly synchronized clocks, which are not used in most off the-shelf devices. Second, the authors assume that packet travel time dominates processing time, which may not be borne out in modern wireless networks, particularly low power wireless sensor networks.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

III. SECURITY IN WIRELESS SENSOR NETWORKS

Today, wireless sensor networks are used for a wide variety of applications: ocean and wildlife monitoring, manufacturing, building safety and earthquake monitoring, and many military applications. An even wider spectrum of future applications may follow, such as monitoring of traffic, pollution, wildfires, building security, water quality, and even people's heart rates. A major benefit of these systems is that they can perform in-network processing to reduce large streams of raw data into useful aggregated information. It is critical to protect this information.

Sensor networks pose unique new challenges which prevent direct application of traditional security techniques. First, to make sensor networks economically viable, sensor devices are limited in their energy, computation, and communication capabilities. Second, in contrast to traditional networks, sensor nodes are often deployed in accessible areas, presenting a risk of physical attacks. Third, sensor networks interact closely with their physical environment and with people, posing new security problems. Consequently, existing security mechanisms are inadequate, and new ideas are needed. Fortunately, these are exciting new problems to inspire research, and there is an opportunity to properly address sensor network security from the start. Security is sometimes considered a stand-alone component of an architecture, where a separate module provides security. This is usually a awed approach. To achieve a secure system, security must be integrated into every component, since components designed without security can become a point of attack. Consequently, security pervades every aspect of system design.

3.1. Trust Setup

When setting up a sensor network, one of the first requirements is to establish cryptographic keys for later use. Key establishment is a well studied problem researchers have proposed a variety of protocols over the past decades. Why can't these key establishment protocols simply be used in sensor networks? The properties of sensor networks render previous protocols impractical. First, many current sensor devices have limited computational power, making public-key cryptographic primitives too expensive. Second, key establishment techniques need to scale to networks with hundreds or thousands of nodes. Third, the communication patterns of sensor networks differ from traditional networks; sensor nodes may need to set up keys with their neighbors and with data aggregation nodes.

3.2. Secrecy and Authentication

Similar to traditional networks, most sensor network applications require protection against eavesdropping, injection, and modification of packets. The standard defense is cryptography. Interesting systems tradeoffs arise when incorporating cryptography into sensor networks. For point-to-point communication, end-to-end cryptography achieves a high level of security, but requires keys set up between all end points and is incompatible with passive participation and local broadcast. Link-layer cryptography with a network-wide shared key simplifies key setup and supports passive participation and local broadcast, but intermediate nodes can eaves drop or alter messages. The earliest sensor networks may use link-layer cryptography, because this provides greatest ease of deployment, but subsequent systems may respond to demands for more security with more so phisticated use of cryptography. Cryptography comes at a performance cost, requiring extra computation and often increasing the packet size. Cryptographic hardware support increases efficiency, but also increases cost.

Recent research demonstrates that software-only cryptography is practical with today's technology; hardware support is not needed to achieve acceptable security and performance levels. For instance, the Berkeley implementation of TinySec incurs only a 5-10% performance overhead using software-only methods. Those experiments also reveal an interesting phenomenon: most of the performance overhead can be attributed to the increase in packet size; in comparison, the cryptographic computations have almost no impact on latency or throughput, since they can overlap with transmission. This puts a limit on how much dedicated hardware will help, because hardware can only reduce the computational costs, not packet sizes.

3.3. Robustness to Communication Denial of Service

Adversaries can severely limit the value of a wireless sensor network by denial-of-service attacks. In the simplest form of denial-of-service attack, an adversary attempts to disrupt operation by broadcasting a high-energy signal. If the

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

transmission is strong enough, the entire system could be jammed. More so- phisticated attacks are also possible: the adversary can inhibit communication by violating the MAC protocol, for instance by transmitting while a neighbor is also transmitting or by continuously requesting channel access with a RTS (request-to-send). One standard defense against jamming employs spread-spectrum communications. However, cryptographically secure spread-spectrum radios are currently not commercially available. Also, this defense is not secure against adversaries who can capture nodes and extract their cryptographic keys. Interestingly, the networked nature of sensor networks allows new, automated defenses against denial of service. When the jamming only affects a portion of the network, a jamming-resistant network could defeat the attack by detecting the jamming, mapping the affected region, and then routing around the jammed area. Further progress in this area may allow for greater security against denial-of-service attacks.

3.4. Secure Routing

Routing and data forwarding is an essential service in sensor networks to enable communication. Unfortunately, current routing protocols suffer from many security vulnerabilities. For example, an attacker can easily perform denial-of-service attacks on the routing protocol, often preventing communication. The simplest attacks consist in injecting malicious routing information into the network that results in routing inconsistencies. Simple authentication can guard against such injection attacks, but some routing protocols are even susceptible to replay by the attacker of legitimate routing messages.

Routing protocols are particularly susceptible to node capture attacks. For instance, researchers have analyzed 14 protocols for routing in sensor networks and found that they are all highly susceptible to node capture attacks: in every case, compromise of a single node suffices to take over the entire network or to prevent communication. It is an open research problem to devise secure routing protocols that are robust against such attacks.

IV. SENSOR NETWORK ATTACKS AND SOLUTIONS

Ad hoc wireless sensor networks (WSNs) promise exciting new applications in the near future, such as ubiquitous on-demand computing power, continuous connectivity, and instantly deployable communication for military and first responders. Such networks already monitor environmental conditions, factory performance, and troop deployment, to name a few applications. As WSNs become more and more crucial to the everyday functioning of people and organizations, availability faults become less tolerable—lack of availability can make the difference between business as usual and lost productivity, power outages, environmental disasters, and even lost lives; thus high availability of these networks is a critical property, and should hold even under malicious conditions. Due to their ad hoc organization, wireless ad hoc networks are particularly vulnerable to denial of service (DoS) attacks and a great deal of research has been done to enhance survivability [8], [10].

While these schemes can prevent attacks on the short term availability of a network, they do not address attacks that affect long-term availability—the most permanent denial of service attack is to entirely deplete nodes' batteries. This is an instance of a resource depletion attack, with battery power as the resource of interest. In this paper, we consider how routing protocols, even those designed to be secure, lack protection from these attacks, which we call Vampire attacks, since they drain the life from networks nodes. These attacks are distinct from previously studied DoS, reduction of quality (RoQ), and routing infrastructure attacks as they do not disrupt immediate availability, but rather work over time to entirely disable a network. While some of the individual attacks are simple, and power draining and resource exhaustion attacks have been discussed before [5], [9] prior work has been mostly confined to other levels of the protocol stack, e.g., medium access control (MAC) or application layers, and to our knowledge there is little discussion, and no thorough analysis or mitigation, of routing-layer resource exhaustion attacks. Vampire attacks are not protocol-specific, in that they do not rely on design properties or implementation faults of particular routing protocols, but rather exploit general properties of protocol classes such as link-state, distance vector, source routing and geographic and beacon routing. Neither do these attacks rely on flooding the network with large amounts of data, but rather try to transmit as little data as possible to achieve the largest energy drain, preventing a rate limiting solution. Since Vampires use protocol-compliant messages, these attacks are very difficult to detect and prevent.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

In our first attack, an adversary composes packets with purposely introduced routing loops. We call it the carousel attack, since it sends packets in circles. It targets source routing protocols by exploiting the limited verification of message headers at forwarding nodes, allowing a single packet to repeatedly traverse the same set of nodes. Brief mentions of this attack can be found in other literature [5], but neither intuition for defense nor any evaluation is provided. In our second attack, also targeting source routing, an adversary constructs artificially long routes, potentially traversing every node in the network. We call this stretch attack, since it increases packet path lengths, causing packets to be processed by a number of nodes that is independent of hop count along the shortest path between the adversary and packet destination. Results show that in a randomly generated topology, a single attacker can use a carousel attack to increase energy consumption by as much as a factor of 4, while stretch attacks increase energy usage by up to an order of magnitude, depending on the position of the malicious node. The impact of these attacks can be further increased by combining them, increasing the number of adversarial nodes in the network, or simply sending more packets. Although in networks that do not employ authentication or only use end-to-end authentication, adversaries are free to replace routes in any overheard packets, we assume that only messages originated by adversaries may have maliciously composed routes.

We explore numerous mitigation methods to bound the damage from Vampire attacks, and find that while the carousel attack is simple to prevent with negligible overhead, the stretch attack is far more challenging. The first protection mechanism we consider is loose source routing, where any forwarding node can reroute the packet if it knows a shorter path to the destination. Unfortunately, this proves to be less efficient than simply keeping global network state at each node, defeating the purpose of source routing. In our second attempt, we modify the protocol from [5] to guarantee that a packet makes progress through the network. We call this the no-backtracking property, since it holds if and only if a packet is moving strictly closer to its destination with every hop, and it mitigates all mentioned Vampire attacks with the exception of malicious flooded discovery, which is significantly harder to detect or prevent. We propose a limited topology discovery period, followed by a long packet forwarding period during which adversarial success is provably bounded. We also sketch how to further modify the protocol to detect Vampires during topology discovery and evict them after the network converges.

V. ISSUES ON SENSOR NETWORK SECURITY

Denial of communication is raised at the routing or medium access control levels. Resource depletion attacks are initiated at the routing protocol layer to permanently disable networks by consuming the battery power. Vampire attacks disrupt the network resources at the routing protocol levels. Stateful (Link state and distance vector) protocols and stateless (Dynamic Source Routing) protocols are verified with attacks. Clean-slate secure sensor network routing protocol is modified to control vampire attacks with resource usage analysis. The following problems are identified in the sensor network security process.

- Low accuracy in damage boundary detection
- Topology discovery is not optimized
- Detection latency is high
- Node energy levels are not considered

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

VI. ROUTING ATTACK DISCOVERY IN WSN

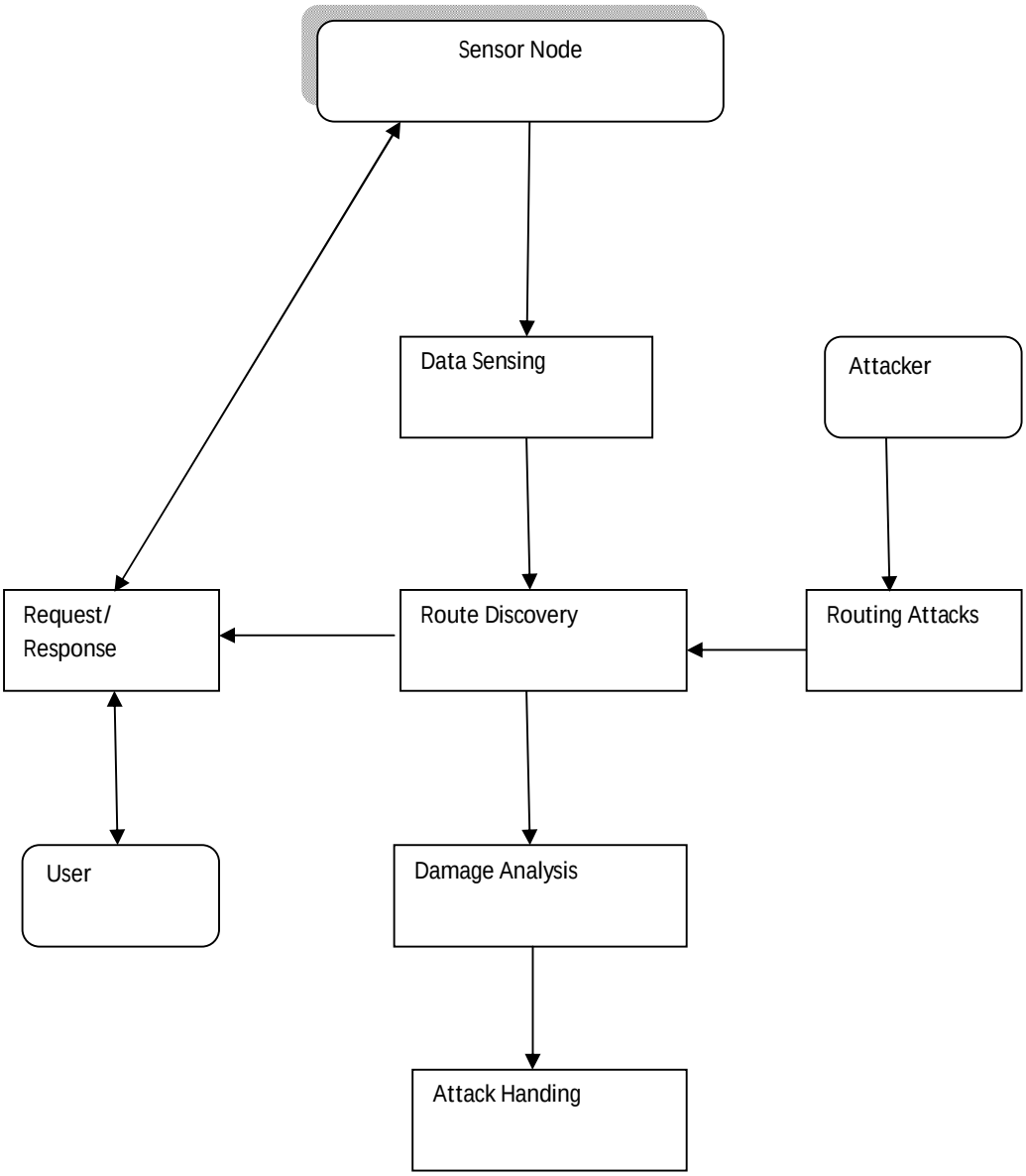

Fig. No: 6.1. Routing Attack Discovery in WSN

Clean-slate secure sensor network routing protocol is improved with optimal boundary estimation model. Topology estimation and packet forwarding prediction is integrated. Transmission coverage factors are integrated with the detection scheme. Energy levels and forwarding packet count information are analyzed to improve the network lifetime.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Wireless sensor network lifetime attacks are controlled with routing analysis. Anonymous routing requests are monitored and detected using the traffic flow details. The system manages the network routing traffic with damage control models. The system is divided into five major modules. They are WSN deployment, data transmission, topology analysis, damage boundary detection and attack handling process.

The sensor network is constructed under the deployment process. Data sensing and transmitting operations are handled under data transmission module. Topology analysis module is used to estimate the network area. Damage boundary analysis module is designed to measure the damage levels. Attack handling module is designed to control routing attacks.

6.1. WSN Deployment

Wireless sensor nodes are placed with a set of deployment schemes. The nodes are placed with reference to the coverage area information. Sensing and transmission coverage details are used in the system. Node initialization is carried out in the deployment process.

6.2. Data Transmission

Sensor nodes perform the data sensing process. The sensed data values are transferred to the requested users. The data values are transmitted using intermediate nodes. Link state routing protocol, Distance vector routing protocol and Dynamic source routing protocols are used for the transmission process.

6.3. Topology Analysis

Topology estimation process is carried out to measure the network area. Coverage information is used in the topology analysis process. Neighborhood details are used to construct the Network Topology Graph for the WSN. Network connectivity details are identified from the topology analysis.

6.4. Damage Boundary Detection

Damage boundary detection process is used to identify the nodes suffered by the attacks. Traffic flow is analyzed to discover the damage boundary details. Node energy details are also considered in the boundary estimation process. Optimal boundary detection algorithm is used for the damage analysis.

6.5. Attack Handling Process

The system detects routing packet attacks under minimum boundary levels. Attackers are detected with reference to traffic probability and energy consumption ratio levels. Attackers requests are dripped immediately by the intermediate nodes. The system issues an alarm message to the boundary level nodes.

VII. CONCLUSION

Wireless sensor network transmission is carried out through the intermediate nodes. Anonymous routing requests are initiated by the attacker nodes. Clean-slate secure sensor network routing protocol is used with security mechanism to control vampire attacks. Boundary detection and topology analysis mechanism is used to improve the detection efficiency. Fault tolerant detection scheme is used in the sensor network security process. Malicious attack controlling model is integrated in the system. Traffic overhead is reduced by the intrusion detection system. Intrusion detection is provided for different deployment schemes under the wireless sensor networks.

REFERENCES

[1] S. Goldberg, D. Xiao, E. Tromer, B. Barak, and J. Rexford, "Path-Quality Monitoring in the Presence of Adversaries," Proc. ACM SIGMETRICS Int'l Conf. Measurement and Modeling of Computer Systems, 2008.
[2] M. Guirguis, I. Matta, and Y. Zhang, "Reduction of Quality (RoQ) Attacks on Internet End-Systems," Proc. IEEE INFOCOM, 2005.
[3] G. Acs, L. Buttyan, and I. Vajda, "Provably Secure On-Demand Source Routing in Mobile Ad Hoc Networks," IEEE Trans. Mobile Computing, Nov. 2006.
[4] X. Luo and R.K.C. Chang, "On a New Class of Pulsing Denial-of-Service Attacks and the Defense," Proc. Network and Distributed System Security Symp. (NDSS), 2005.
[5] B. Parno, M. Luk, E. Gaustad, and A. Perrig, "Secure Sensor Network Routing: A Clean-Slate Approach," CoNEXT: Proc. ACM CoNEXT Conf., 2006.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

[6] D.R. Raymond and S.F. Midkiff, "Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses," IEEE Pervasive Computing, vol. 7, no. 1, pp. 74-81, Jan.-Mar. 2008.
[7] Eugene Y. Vasserman and Nicholas Hopper, "Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor Networks", IEEE Transactions On Mobile Computing, February 2013.
[8] J. Deng, R. Han, and S. Mishra, "Defending against Path-Based DoS Attacks in Wireless Sensor Networks," Proc. ACM Workshop Security of Ad Hoc and Sensor Networks, 2005.
[9] D.R. Raymond, M.I. Brownfield, and S.F. Midkiff, "Effects of Denial-of-Sleep Attacks on Wireless Sensor Network MAC Protocols," IEEE Trans. Vehicular Technology, Jan. 2009.
[10] J. Deng, R. Han, and S. Mishra, "INSENS: Intrusion-Tolerant Routing for Wireless Sensor Networks," Computer Comm., 2006.
[11] L. Xiaojun, N.B. Shroff, and R. Srikant, "A Tutorial on Cross-Layer Optimization in Wireless Networks," IEEE J. Selected Areas in Comm., pp. 1452-1463, Aug. 2006.