International Journal of Trend in Scientific Research and Development (IJTSRD)
International Open Access Journal
ISSN No: 2456 - 6470 | www.ijtsrd.com | Volume - 2 | Issue – 4

A Study on Security in Wireless Sensor Networks

[1]Rashmi, [2]Sumit Dalal, [3]Shabnam Kumari
[1]M.Tech Scholar, [2,3]A.P
[1,2]Dept of ECE, [3]Department of CSE,
[1,2,3]Sat Kabir Institute of Technology & Management, Bahadurgarh, Haryana, India

Abstract- Wireless Sensor Networks (WSNs) present myriad application opportunities for several applications such as precision agriculture, environmental and habitat monitoring, traffic control, industrial process monitoring and control, home automation and mission-critical surveillance applications such as military surveillance, healthcare (elderly, home monitoring) applications, disaster relief and management, fire detection applications among others. Since WSNs are used in mission-critical tasks, security is an essential requirement. Sensor nodes can easily be compromised by an adversary due to unique constraints inherent in WSNs such as limited sensor node energy, limited computation and communication capabilities and the hostile deployment environments.

Keywords- *WSN, WTE, SN, FN, MAC*

I. INTRODUCTION

Wireless sensor network (WSN) consists of a large number of spatially distributed autonomous sensor nodes working cooperatively to monitor the surrounding physical phenomena or environmental conditions (monitored target) and then communicate the gathered data to the main central location through wireless links. A sensor node, also known as mote is defined as a small, low-powered, wireless device, capable of gathering sensory information, perform limited data processing and transmit the gathered information to other nodes in the network via optical communication (laser), radio frequencies (RF) or infrared transmission media. A sensor node senses physical phenomena like light, temperature, humidity, pressure, chemical concentrations and any other phenomenon capable of cau-sing the transducer respond to it. Once the phenomena is sensed, the data collected (measurement) is converted into signals for further processing to reveal some characteristics pertaining the phenomenon from the target area (Hussain, et al., April, 2013). Several schemes for malicious nodes detection and isolation in WSN have been proposed. This research explores and improves one of them, the Weighted Trust Evaluation (WTE) Scheme. WTE is a lightweight algorithm use in a three-layer hierarchical network architecture consisting of low-powered Sensor Nodes (SN) having limited capabilities, higher-powered Forwarding Nodes (FN) which collect data from the lower layer (SNs) and the Base Stations (BS) or Access Points (AP) layer that route information between the wireless sensor network (WSN) and the wired infrastructure. Weighted Trust Evaluation Scheme is based on several assumptions i.e. both Forwarding Nodes (FNs) and Base station (BS) are trusted and won't be compromised and that the number of normal working nodes exceeds the compromised nodes. (Sumathi & Venkatesan, 2014) [1] Once an adversary gains control over the BS then it leads to create any possible attacks in the network. The threat of Forwarding Nodes being compromised is not considered, a compromised FN gives an adversary control of all the sensor nodes under it. In this research, we propose an enhanced WTE based detection algorithm that aims to address the drawback of the WTE scheme by employing STL. The STL will come in handy to address the threat of the compromised forwarding nodes and since there are few, issues of congestions and delays in the network are avoided.

II. LITERATURE REVIEW

Several schemes for malicious node detection and isolation in WSNs have been proposed. It is critical to detect and isolate the compromised nodes in order to avoid being misled by the falsified information injected by the adversary. Luo et al. [19] have pointed out that infrastructureless ad hoc networks rarely have a real defense mechanism against most of the attacks, including both outsider and insider attacks such as compromised node attacks. They suggested a system design like this – if one node is named trusted by certain number of its neighboring nodes, that particular node is trusted both locally and globally. However, since the system uses a minimum number of trusted nodes it is not so applicable to sensor networks where the nodes are randomly spread out. In other words, it is possible that under certain conditions nodes cannot find the minimum number of neighboring nodes in order to be named trusted.

Sung & Choi, (2013) [2] Proposed a Dual Threshold technique for malicious node detection that employs two thresholds to minimize false alarm rate as well as improve the detection accuracy. All deployed sensor nodes do have transmission ranges, 'tr', and any other sensor node in close proximity i.e. within the node transmission range is considered its neighbor. Each individual sensor node maintains its neighbors' trust values to designate their trustworthiness. The sensor node makes a localized decision based on its own readings and those of its neighbors taking into account their trust values. Trust values lie between 0 and 1. If Tik=0 means node Ni does not trust Nk at all. A node also has its own trust value, once Tii=0 means the node is faulty.

(Curiac, et al., 2007) [3] Proposed Auto regression Technique which is a mechanism that relies on past/present sensor node values. The sensor node present value is compared with an estimated value computed from its own previous values by an autoregressive predictor placed at the base station. The two values are compared to check if node behavior is normal or abnormal. If the variance between these two values is higher than a set threshold, the node is regarded malicious.

(Yang, et al., 2007) [4] Proposed SoftWare-based ATTestation (SWATT) mechanism to authenticate the embedded device (sensor nodes) memory contents and detect any falsification or maliciously altered or inserted code in memory. The verifier send to the embedded device a randomly generated MAC key, which then calculates Message Authentication Code (MAC) value on the whole memory using the received key and returns the MAC value. The verifier uses the checksum to verify the memory contents. If the memory has been maliciously altered by the adversary then the checksum is false.

(Bao, et al., 2011) [5] Proposed a Trust-Based Intrusion Detection approach which considers a composite trust metric derived from both social trust and quality of service (QoS) trust to identify malicious nodes in the wireless sensor network. The cluster head apply intrusion detection in the sensor nodes to assess the trust worthiness and maliciousness of the nodes in its cluster. This is achieved by statistically examining peer-to-peer trust evaluation results gathered from the different sensor nodes (Sumathi & Venkatesan, 2014).

(Nidharshini & Janani, December 2012.) [6] Proposed a Sequential Probability Ratio Testing (SPRT) to detect duplicate nodes made by an adversary in the WSN. The attacker can easily capture and make replicas of unattended nodes and then use them to take control of the entire network. The base station is responsible for identifying compromised nodes by computing the speed of observed sample nodes and decides which nodes' speed exceeds the decided threshold speed, these ones are regarded malicious.

1. Security Goals for Wireless Sensor Networks

The main objectives of Wireless Sensor Networks (WSNs) security are as follows:

A. Data Confidentiality

Confidentiality refers to the ability to conceal vital messages' content from being disclosed to unauthorized party or protect the messages against unintended access. Sensor nodes may exchange or pass highly sensitive information such as cryptographic key distribution and it must therefore remain confidential. This means that it is very crucial to build a secure communication channel in a sensor network. Data encryption should also be used to secure the data being transmitted across the sensor network.

B. Data Integrity

Data integrity is referred as the ability to assert that the message was not altered, tampered with or improperly modified in transit by an adversary. It is essential to guarantee data reliability.

The sensor network integrity will be compromised when (Padmavathi & Shanmugapriya, 2009) [7]: A malicious node in the network injects incorrect and misleading data. Unstable and turbulent conditions resulting from the wireless communication channel causing data damage or loss. (Akykildiz, et al., 2002) [8].

C. Data Authenticity

Authentication ensures the reliability of the received message through source identity verification. An attacker can alter the data packet or even modify the whole packet stream by introducing extra bogus packets. Data authentication is therefore needed so that the recipient node can confirm that the data actually originates from the claimed sender (correct source).

D. Data Availability

Availability seeks to ensure that the required network services are functioning at a desired level of performance and work promptly in normal situations as well as in the event of attacks or environmental mishaps. It implies that the sensor node has the ability to access and utilize the available resources and that the network is operational and ready for use to transmit messages.

E. Data Freshness

This ensures that the transmitted messages are current and old content (expired packets) are not replayed by an adversary to either mislead the network or keep the network resources busy thereby reducing the sensor network vitality. It is essential especially in shared-key design strategies that require the keys be changed over time. (CHELLI, 2015) [9].

F. Secure Localization

Sensors may get displaced during their deployment, after a certain length of time or after a critical displacement incident. WSN operations depends on its ability to automatically and accurately locate each sensor node in the network after the displacement. (CHELLI, 2015) [9].

G. Self-Organization

WSN being an ad-hoc network and lacking a fixed infrastructure for network management requires that each node be independent and versatile so as to be able to self-organize and self-heal depending on the various situations, topology and deployment strategy. This inherent feature of the sensor network is a great challenge to WSN security. If self-organization is absent in a wireless sensor network, an attack or the risky deployment environment may have dire consequences. (Padmavathi & Shanmugapriya, 2009) [7]

G. Time Synchronization

Time synchronization is required by many WSN applications, it is essential in multi-hop communication, conservation of node energy (periodic time sleep) and node localization. Sensor nodes may wish to determine the network latency of a packet as it transits between a pair of sensor nodes (sender-receiver) (Padmavathi & Shanmugapriya, 2009) [7]. Collaborative time synchronization may be needed by wireless sensor network for tracking applications.

III. ATTACKS LAUNCH FROM MALICIOUS SENSOR NODES

Since the wireless sensor networks are set up in hostile environments, sensor nodes can be compromised easily by the adversary due to the resource constraints such as limited memory space, battery lifetime and computing capability. Detection and isolation of these compromised nodes is crucial to avoid being deceived and misguided by falsified data injected by the attacker.

An adversary can easily launch a range of attacks against the wireless sensor network through the compromised (malicious) nodes Some of the attacks that can emanate from malicious nodes include sinkhole attacks, black hole attack, wormhole attack, Sybil attack, HELLO flooding attacks and Denial-of-Service attacks. (Atakli, et al., 2008)

A. Denial-of-Service attacks

Denial of Service (DoS) attack refers to an explicit attempt by the adversary to deny the victim (legitimate user) use or access to all or part of their network resources (Soomro, et al., 2008) [10]. In a DoS attack an adversary may destroy or disrupt a network, the attacker can also overload the network with bogus requests thereby diminishing the network's ability to provide a service (Virmani, et al., 2014) [11] . These attacks make the sensor node depletes the battery power and degrade the overall sensor network performance.

B. Black Hole attack

A malicious node take advantage of routing protocol's packet route discovery process vulnerabilities to advertise itself to other nodes in the sensor network as having the shortest valid route to the packets destination node (Y-C & Perrig, 2004) [12]. The attack modifies the routing protocol so as to channel traffic through a particular node (malicious node) controlled by the adversary.

In the route finding process, the source node relays RREQ (Route Request) packets to intermediate forwarding nodes to find the best valid route to the intended packet destination node. Since malicious nodes do not consult the routing table, they reply immediately to the source node. (Das, et al., 2002) [13] . The source node then assumes that the route finding process is over, ignores other nodes' RREP (Route Reply) messages and selects the route through the malicious node as the best route to transmit the data packets to the intended destination. The malicious node is able to accomplish this by allocating a high sequence number to the RREP packet. The source node starts forwarding its packets to the black hole trusting that they will be relayed to the destination. The adversary controlling the black hole may now discard these packets instead of relaying them to the destination node as stipulated by the protocol.

C. HELLO Flood attack

A laptop-class adversary with a higher radio transmission power and range relays routing protocol HELLO packets to a number of other sensor nodes within a WSN making them assume the attacker is their neighbor (Padmavathi & Shanmugapriya, 2009) [7]. The hello packets recipient sensor nodes are influenced that the compromised node (adversary) is within their radio range. These node during data transmission to the base station may forward packets to the adversary since they assume it is their neighbor and are eventually spoofed by the adversary.

Hello flood attack could be mitigated using pairwise authentication of nodes or by employing geographic routing protocols. Pairwise authentication enable sensor nodes verify bi-directionality of a link before they can construct routes to forward traffic received over the link. Geographic routing protocols like Geographic and Energy-Aware Routing allow nodes discard hello messages received from nodes not within their communication range in terms of locations, which nodes broadcast to each other (Raymond & Midkiff, 2008).

D. Sink hole attack

In a sinkhole attack, the attacker's main goal is to allure the traffic from nodes in its close proximity (neighboring nodes) through a compromised sensor node. These attacks make the compromised attacking node look enticing and ideal to be used by the surrounding neighboring nodes to forward traffic. (Padmavathi & Shanmugapriya, 2009) [7]

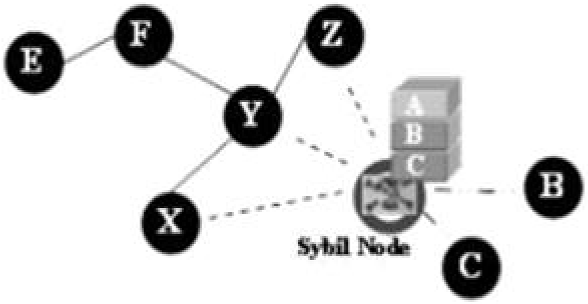

Figure 1: Sinkhole Attack (Alajmi, July 2014)

E. Sybil attack

Sybil attack is an identity-based attack in which an attacker infects a single node with malicious code that duplicates the node; presenting multiple identities in multiple locations to other nodes in the sensor network. The multiple identities of node degrades the integrity of data as well as straining the network's resources. The Sybil attack decreases the efficiency of fault tolerant schemes like multipath routing, distributed storage and topology maintenance (Padmavathi & Shanmugapriya, 2009).

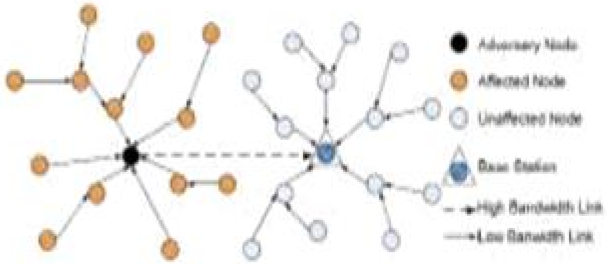

Figure 2: Sybil Attack (Alajmi, July 2014)

Authentication and encryption schemes can protect a sensor network from Sybil attacks.

F. Worm Hole attacks

This is an attack in which the packets or their individual bits are captured at one part of the sensor network, tunneled over a low latency link to another location and are then replayed at their destination location (Hu, et al., 2003). This is usually accomplished by two distant colluding nodes which create an impression that the two locations involved are directly connected even though they are genuinely distant (Virmani, et., 2014)[11].

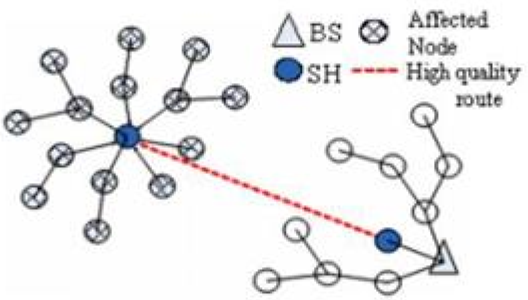

Figure 3: Wormhole attack (Abdullah, et al., 2015) [14]

A wormhole attack involves two distant malevolent nodes conspiring to understate their inter-node distance by relaying packets through an out-of-bound channel which is only available to the adversary.

Some defense strategies against wormhole attacks are packet leashes which ensures that packets are not accepted "too far" from their source. Geographical leashes uses GPS information embedded into the packet being send whereas temporal leashes uses the nodes' clocks timestamps added to the packet.

IV. MALICIOUS NODES DETECTION TECHNIQUES

Several schemes for malicious node detection and isolation in WSNs have been proposed.

A. Weighted Trust Evaluation Scheme.

Weighted-Trust Evaluation (WTE) based scheme is a light-weighted algorithm used to detect and subsequently isolate compromised (malicious) nodes by monitoring their reported data in a hierarchical WSN architecture. (Zhao, et al., March 2013) [15] (Atakli, et al., 2008) [17] Employed and demonstrated this method using a three-layer hierarchical sensor network. The components of the three-layer hierarchical network architecture are:

[2] Low-power Sensor Nodes (SN) whose functionalities are limited. SN is in the lowest tier and does not offer multi-hop routing capacity as in a traditional flat sensor network. SNs report the data to its Forwarding Node.

[3] Higher-power Forwarding Nodes (FN) which collect data from the lower layer (SNs), verify its correctness, aggregate and forward it to other FNs or to the upper layer (Base Station).

[4] Base Stations (BS) or Access Points (AP) which verifies data reported by the FNs as well as routing data between the wireless sensor network and the wired infrastructure.

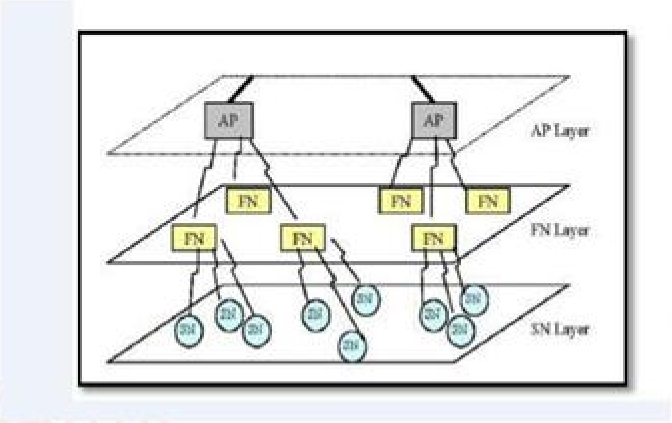

Figure 4: Architecture of the hierarchical WSN (Atakli, et al., 2008)[17]

This scheme is based on two assumptions; first, the FNs and Base station are trusted nodes that cannot be compromised by an attacker since once an adversary seize control of the BS then they can launch any possible attack in the sensor network (Sumathi & Venkatesan, 2014) [1] (Hu, et al., 2009) [16] (Atakli, et al., 2008) [17]. Another critical assumption is that the normal nodes (working in proper condition) in the sensor network exceeds in number the compromised nodes. Otherwise, the scheme may misidentify normal node as compromised nodes increasing false positives. The proposed enhanced WTE intends to detect and isolate malicious FNs in the sensor network instead of assuming they won't be compromised by adversaries. This aims to cautions all the SNs under a FN which the attacker can control and manipulate once it take control of a particular FN.

a. Malicious Nodes Detection

A compromised sensor node provides falsified information that may wrongly mislead the senor network. This problem is referred as the Byzantine problem. A compromised/malicious sensor node can continuously forward wrong information to the upper layers. The aggregator (AP or FN) in the upper layer may compute an incorrect aggregation result due to the misleading information emanating from the malicious nodes. This may have disastrous effects to the decision making process.

WTE scheme models malicious node detection and isolation in 2 steps;

First, an initial weight Wn is assigned to every sensor node (SN) in the sensor network. The Forwarding Node (FN) gathers all the reported data from all the SNs under it and computes an aggregated result taking into account each SN weight.

$E = \sum_{=1} / \sum_{=1}$

Where:

E = FN aggregate result.

Wn = SN assigned weight (Ranging between 0 and 1).

Un = SN output information (Un is usually dependent on the sensor network application. The output value may be "true" or "false" or continuous numbers like in a case of temperature readings).

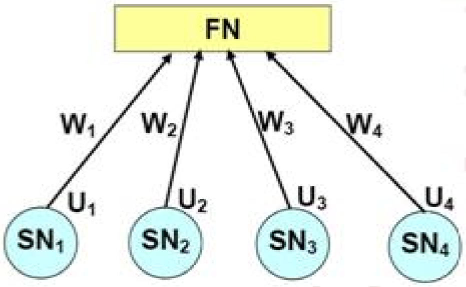

Figure 5: Weight-based hierarchical wireless sensor network (Atakli, et al., 2008) [17].

Each SN weight is updated based on the accuracy of the reported information. The SN weight is updated for two reasons. First, if a compromised sensor node continuously forward data that is inconsistent with the final aggregate decision, its weight is likely to be reduced by a set weight penalty. If the weight decreases below a given threshold, then it is identified as a malicious node. Second, the SN weight determine how much a sensor node report contribute to the final aggregate decision. This is meant to lower the effect of incorrect reports from malicious sensor node.

b. Weight Value Recovery

The SN weight is decreased by a certain penalty value once it is detected to be reporting falsified data. However, the false report may be a result of a temporary communication channel interruption and the SN is neither malicious nor faulty. The weight values for such SNs needs to be recovered after the disturbance rather than keeping these values low permanently. The SNs that behave correctly thereafter longer than a set recovery time have their weight value increased.

B. Stop Transmit and Listen (STL)

The STL scheme employs non-transmission time slots to detect malicious nodes. Each sensor node have an inbuilt time limit to stop their data transmissions and listen for traffic. Once the nodes have been deployed and they have started sensing the target phenomena, the sensed data is sent to the base station. After every few seconds or after a set transmission time, each sensor node halt their data transmission process and listens for malicious traffic. If a sensor node transmits data during the non-transmission time (listening time) , it is caught by its neighbor nodes in the sensor network and it is regarded malicious as it exhibits malicious behavior. If a malicious node doesn't transmit data during a non-transmission time slot, it will still be caught in other frequent non-transmission times. The malevolent behavior of a malicious node is broadcasted across the entire sensor network. (Sathyamoorthi, et al., 2014) [18]. Then every other sensor network node desist from either forwarding data to the detected malicious node or accepting from it.

This technique has some weaknesses such that when the whole network or a major portion of it stopped their transmission at a time (during non-transmitting time) and then resume transmission, congestion and unwanted delay in the network operations arises (Sumathi & Venkatesan, 2014) [1].

2. CONCLUSION

One of the important problems that are related to the use of wireless sensor networks in harsh environments is the gap in their security. This paper provides information about various security goals in WSN. Then paper elaborates the Attacks that launch from Malicious Sensor Nodes and various techniques available for the above purpose have been discussed.

References

[1] Sumathi , K. & Venkatesan, D. M., 2014. A Survey on Detecting Compromised Nodes in Wireless Sensor Networks. (IJCSIT) International Journal of Computer Science and Information Technologies, Volume 5, pp. 7720-7722.

[2] Sung, . Y. L. & Choi, Y.-H., 2013. Malicious Node Detection Using a Dual Threshold in Wireless Sensor Networks. Journal of Sensor and Actuator Networks.

[3] Curiac, D.-I.et al., 2007. Malicious Node Detection in Wireless Sensor Networks Using an Autoregression Technique. Athens, Greece, s.n.

[4] Yang, Y., Wang, X., Zhu, S. & Cao, G., 2007. Distributed Software-based Attestation for Node Compromise Detection in Sensor Networks. Pennsylvania, s.n.

[5] Bao, F., Chen, I.-R., Chang, M. & Cho, J.-H., 2011. Trust-Based Intrusion Detection in Wireless Sensor Networks. Kyoto, Japan, s.n.

[6] Nidharshini, T. & Janani, V., December 2012.. Detection of Duplicate Nodes in Wireless Sensor Networks Using Sequential Probability Ratio

Testing. International Journal of Advanced Research in Computer and Communication Engineering, 1(10).

[7] Padmavathi, . D. . G. & Shanmugapriya, M. D., 2009. A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks. International Journal of Computer Science and Information Security,, Volume 4.

[8] Akykildiz, . I. . F., Su, W., Sankarasubramaniam, Y. & Cayirci, E., 2002. A Survey on Sensor Networks. IEEE Communication Magazine.

[9] CHELLI, K., 2015. Security Issues in Wireless Sensor Networks:Attacks and Countermeasures. Proceedings of the World Congress on Engineering 2015, Volume 1, pp. 1-6.

[10] Soomro, S. A., Soomro, S. A., Memon, A. G. & Baqi, . A., 2008. Denial of Service Attacks in Wireless Ad-hoc Networks. Journal of Information & Communication Technology, Volume 04, pp. 01-10.

[11] Virmani, D., Soni, A., Chandel, S. & Hemrajani, M., 2014. Routing Attacks in Wireless Sensor Networks: A Survey. Bhagwan Parshuram Institute of Technology, India.

[12] Y-C , H. & Perrig, A., 2004. A Survey of Secure Wireless Ad Hoc Routing. IEEE Security and Privacy.

[13] Das, R., Purkayastha, D. B. S. & Das, D. P., 2002. Security Measures for Black Hole Attack in MANET: An Approach. Proceedings of Communications and Computer.

[14] Abdullah, M. I., Rahman, M. M. & Roy, M. C., 2015. Detecting Sinkhole Attacks in Wireless Sensor Network using Hop Count. I. J. Computer Network and Information Security, p. 51.

[15] Zhao, S., Tepe, K., Seskar, I. & Raychaudhuri, D., March 2013. Routing Protocols for Self-Organizing Hierarchical Ad Hoc Wireless Networks. Proceedings of the IEEE Sarnoff Symposium, Trenton, NJ,

[16] Hu, H. et al., 2009. Weighted trust evaluation-based malicious node detection for wireless sensor networks. Int. J. Information and Computer Security, 3(2), p. 148.

[17] Sathyamoorthi, T., Vijayachakaravarthy, D., Divya, R. & Nandhini, M., 2014. A SIMPLE AND EFFECTIVE SCHEME TO FIND MALICIOUS NODE IN WIRELESS SENSOR NETWORK. International Journal of Research in Engineering and Technology, 03(02)