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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 11, November 2013

A NOVEL ARCHITECTURE FOR MITIGATING THE MANET ROUTING ATTACKS

Yamini.T[1], A.Sudhir Babu[2]

M.Tech Student, CSE Department, PVP Siddhartha Institute of Technology, Vijayawada, AP, India [1]

Associate Professor, CSE Department, PVP Siddhartha Institute of Technology, Vijayawada, AP, India [2]

Abstract: A mobile ad hoc network is a network with many free or autonomous nodes comprised of mobile devices or mobile pieces that arrange themselves in different ways operating without specific network administration. Mobile Ad Hoc Network (MANET) is unique by virtue of its self configuring and optimizing nature. Due to its flexible nature MANET is exposed to different types of attacks, mainly routing attacks. Attack Prevention methods like encryption, intrusion detection system, intrusion prevention system can be used for reducing certain attack possibilities. An Intrusion detection system monitors and analyses the activities of the nodes and determines the performance with the security rules. It also alerts the neighboring nodes if irregularity has been detected in the performance of a node. An intrusion Response System recovers the affected services and reconfigures the system. As topology of MANET changes continuously achieving security in these networks is very difficult.

Keywords: Ad hoc networks, intrusion detection system, intrusion response, routing attacks.

I. INTRODUCTION

Mobile Ad Hoc Networks (MANET) is distributed and self configuring wireless network. MANET does not have a predefined network infrastructure. Application of MANET is benefited in areas such as military services, disaster relief and mine site operations. Each node communicates with the other acting as routers. The co-operation and trust between the nodes are depended for the proper functioning of this network. Since the network topology in MANET changes unpredictably and rapidly it is highly vulnerable to various kinds of attacks. Attack prevention methods such as intrusion detection system, intrusion prevention, authentication and encryption can be used in defence for reducing certain attack possibilities. MANET is considered one of the most promising fields in research and development of wireless networks. There exist many intrusion response mechanisms for routing attacks. The existing techniques usually attempt to isolate the malicious nodes from the topology there by causing the partition of network topology.

Techniques such as binary responses may result in unpredicted network partition, causing supplementary damages to the network infrastructure and naive fuzzy responses could lead to ambiguity in countering routing attacks

Many intrusion detection methods have been proposed for discovering the malicious nodes and preventing the neighbour nodes from the malicious nodes. Although several mechanisms and routing protocols exist, each one of them has one or more vulnerabilities. Implementation of MANET has become a massive amount of task to be done.

On identifying a malicious node, it has either to be repaired or another new route must be recognized. In most of the available techniques, when malicious node is identified, it is completely isolated from the network, making network partitions, causing communication problem. The above information provides brief detail about MANET & routing attacks. The paper is structured as follows. Chapter II gives a study on various intrusion response techniques used. Chapter III explains table with comparison of these existing systems. In Chapter IV we conclude the process.

II. EXISTING TECHNIQUES

Several mechanisms have been proposed for better performance of MANET. These methods include detection, [4], [10] prevention and evaluation of different types of attacks and malicious nodes. The main aim of Intrusion response system is to recover affected nodes and to reconfigure them. Some of the intrusion response methods used in MANET is discussed below:

A. Trust Modelling and Evaluation of Nodes

As there is no central authority involved, the performance of ad hoc networks purely depends on cooperation and trust among distributed nodes.

Reliability of nodes is evaluated in order to provide security in ad hoc networks. For this we quantitatively measure trust and model trust propagation in ad hoc networks. Trust is a

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 11, November 2013

relationship between two entities. In [1] one entity trusts other to perform action. The source node is denoted as subject and the intermediate node as the agent and is denoted as {subject: agent, action}. A real number called the trust value is used to measure the level of trust. Trust relation does not be symmetric i.e., node A trust B doesn't means B trust A. Four basic axioms are presented for establishing the trust relationship.

- Axiom1: trust is measured by uncertainty. Trust describes whether the agent will perform action in view point of a subject.

- Axiom 2: trust is not increased by concatenation propagation. When subject establishes trust through a third party recommendation with an agent, its value between subject and agent should not be more than subject and recommenders trust value as well as recommender and the agent

- Axiom 3: Multipath propagation of trust does not reduce trust. If the subject receives the same recommendations for the agents from multiple sources, the trust value should be no less than that in the case where the subject receives less number of recommendations.

- Axiom 4:Trust derived from multiple recommendations from a single source should be less than that from independent sources

There are two trust models: entropy- based and probability based. Trust values are coupled with two actions: packets forwarding and getting recommendations. Every node maintains trust record, a recommendation buffer and an observation buffer.

When a node A wants to know route to node D, it finds multiple routes to D. To obtain trust recommendation, node A checks its trust record and obtains a set of trusted nodes S. Every node finds trustworthiness of route nodes from its own Trust record, there after updates their trust record based on the observation of route quality. Thus establishment of trust recommendation leads to traffic overhead and delay.

Time to live (TTL) field is used in TRR message to reduce overhead and nodes work based on TTL time. Routing protocol used is Dynamic Source Routing (DSR) [13]. Based on axioms, observations and through propagation the level of trustworthiness is quantitatively measured. Two models that regulate concatenation and multipath propagation are developed. A distributed system is designed to obtain, maintain and to update trust records related with nodes behaviour in forwarding packets and making recommendations about other nodes. By this we can detect type of malicious node and its behaviour their by mitigating the risk of its presence in the network.

B. Reputation Management in Ad Hoc Networks

Co-operation among nodes is enforced through Reputation management [2], [12] systems in ad hoc networks. This reputation is used in evaluating, detecting and reasoning the nodes behaviour. Based on this evaluation, nodes are recognized as either cooperative or malicious nodes & Sequential Probability Ratio Test is used in [2] for this purpose. The SPRT is a specific sequential hypothesis test. SPRT evaluates node behaviour by distinguishing it with node's behaviour [3]. A node is chosen as Cooperative behavioring node if it forwards all packets successfully. But in certain conditions such as in high congestion and in channel failure it may not route packets successfully. In such case we make wrong assumption about the behaviour of cooperating node. Hence, behaviour of nodes varies from time to time due to changes in local and network-wide conditions. Thus affects the ability of reputation management method to distinguish between a nodes decision whether to forward packet and in its inability to do so in such adverse condition. In this method we evaluate nodes behaviour in a time slot manner varying slots according to the congestion and channel impairment. This method mainly depends on two premises

1) A thorough observation of the node behaviour when there is less traffic which helps to identify the co operation of nodes at normal time.
2) The node behaviour is assessed based on a comparison with its own behaviour.

This method takes into consideration the misbehaviour selfish node. This node intentionally not participates in forwarding of packets to preserve its resources such as power consumption. This node may drop packets forwarded through it. Packet forwarding ratio is used as a metric to evaluate the node behaviour. Packet forwarding (FWD) ratio and packet request (RCV) are monitored by the node. The function of node reputation is illustrated in Fig.1.

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 11, November 2013

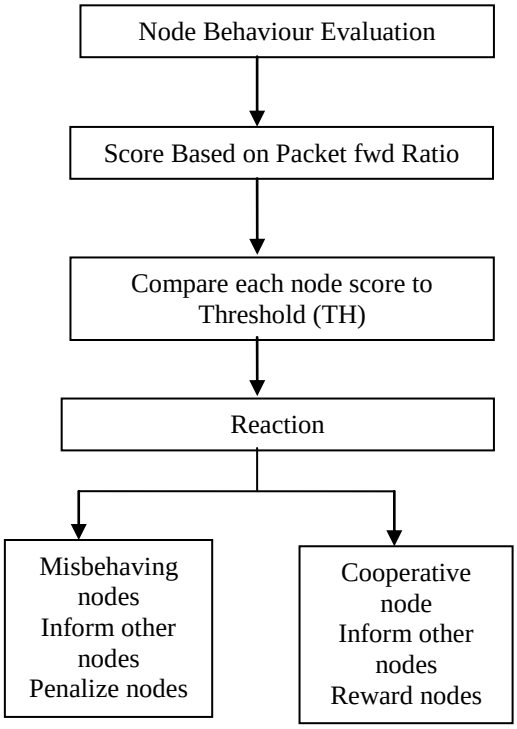


Fig.1. Function of Reputation Management

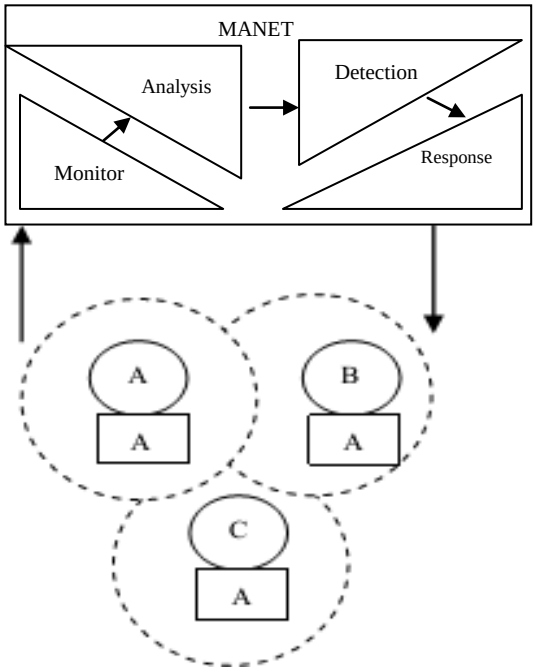


Fig.2. ADRS in MANET

There is no communication overhead in this approach as there is no exchange of observation between nodes. Every node observes RCV, FWD, DRP events which give neighbouring nodes behaviour. Each node acts in promiscuous node and distinguish data packets that reflect RCV or FWD events related to its neighbours.

Every node then stores packet traces for data packets that reflect RCV event in a lookup table to identify any subsequent FWD events. Each RCV event in lookup table is associated with time-out value. If an FWD event is not noted within the specified time-out period, DRP event is trigged and corresponding RCV event is purged.

C. Anomaly Detection and Response System (ADRS)

In Mobile Ad hoc Networks anomalous events are analysed using Anomaly Detection and Response systems. In MANET autonomous nodes work independently and cooperatively with each other. These nodes are distinguished from other network counter parts using function roles such as: self-configuration, self-healing, self- optimization and self-protection [4]. ADRS analyses the MANET anomalies resulted by both intentional and unintentional or accidental attacks such as traffic congestion, signal interference etc. ADRS monitors node performance and analyses its behaviour and makes responses corresponding to the analysis.

Each Anomaly Detector (AD) in an ADRS monitors the behaviour and traffic of the neighbouring nodes and shares the information between the other AD's. The overhead is negligible due to light weight of AD's. Packet Forwarding Ratio determines the behaviour of the node. Major parameter that determines node behaviour is based on threshold value which determines the distance between regularity of monitored events and that of normal profiles.

ADRS is evaluated using detection accuracy and false positive rate. Operational costs including both detection cost and response cost are important factors but are ignored. This metric is important in MANET as its nodes usually have scarce resources and an ADRS consuming non-negligible overhead would be undesirable. As each network node is autonomous, they may refuse to run an ADRS sensor if the overhead impedes its normal operations. From a systematic viewpoint, it is a significant issue to explore the trade off between detection performance and operational cost [11] (and other metrics) of an ADRS, so that the best detection performance can be achieved with the minimum operational cost.

The ADRS deployed in Fig 2 specifies the following details:

- Every AD monitors local traffic and nodes behaviour and shares this information with other Ads for correlating events and coordinating responses against an observed anomaly.
- AD varies in detection coverage and blind spot impacted by both detection algorithms and observations.
- AD provides negligible overhead, hence it is light weight
- Each AD is expected to capture the drifts of a node's normal profile, thus enabling ADRS to adapt to the dynamic

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 11, November 2013

network environment.

- ADRS is expected to be operating in secure and dependable manner, avoiding the introduction of new vulnerabilities which may allow sophisticated attackers to compromise ADRS. Also, the failure of AD does not result in performance deterioration of the whole ADRS.

The framework allows to make the operation ADRS as a distributed optimization problem, aiming to get the best tradeoffs between operational metrics. Rather than relying on specific anomaly detection algorithms and architectures, the framework lays a theoretical foundation for any ADRS to achieve cost sensitive detection and response by adjusting the ADs behaviour.

D. Watchdog and Pathrater

In Ad hoc networks throughput is an important factor and increasing throughput we can increase quality of communication. Two methods Watchdog and Pathrater are being used here.

Watchdog is a method used to find malicious or misbehaving node, whereas Pathrater guides the routing protocols to avoid these identified malicious nodes by providing another path. By employing these two techniques together in a network, throughput increases by 17% when there are 40% of malicious nodes. These two methods are extended to Dynamic Source Routing (DSR) algorithm to reduce the number of misbehaving nodes in a network. Watch dog detects the neighbouring nodes' behaviour by listening to them. If any node doesn't forward the packet, that node will be considered as misbehaving node. Fig 3.explains how a watch dog works

Fig.3 Watchdog

When node A wants to send packet to node S it can't transmit packet all the way to S. instead A uses intermediate nodes B and C. Node B can listen to node C whether it is transmitting packet to node S. A buffer is maintained at each node where recently sent packet is stored. This is compared with each packet overhead to see if there is any match. If a packet remains in the buffer for longer than a certain timeout, watch dog increments a failure tally for the node responsible for forwarding on the packet. When tally exceeds a certain threshold bandwidth, it identifies that the node is misbehaving and sends a message to the source node informing about the misbehavioring node.

Pathrater works by the information from the Watch dog. It selects the most reliable path for the nodes to communicate. It will have a node rating, basing on which path reliability is calculated. Pathrater cannot detect misbehaviour nodes without an active Watch dog. Pathrater [5] assigns ratings to nodes according to the following algorithm. When pathrater knows node behaviour (through route discovery) it assigns it a "neutral" rating of 0.5. Rating of 1.0 is used to rate a node by itself.

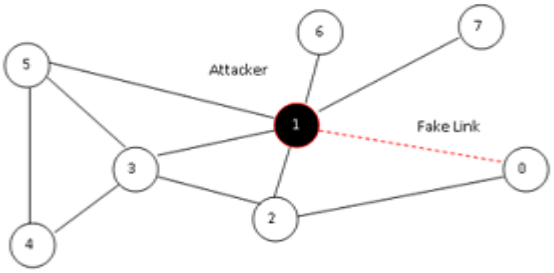
When calculating path rates, if all other nodes are neutral rather than suspected misbehaving node(s), the pathrater picks the shortest path length. At periodic intervals of 200ms Pathrater increments rating of nodes on all actively used paths by 0.01.

Actively used path is one on which the node has sent a packet in the incremental time interval specified previously. A neutral node can attain a maximum value of 0.8. A node's rating is decremented by 0.05 when a link break during packet forwarding is detected and the node becomes unreachable. The lower bound rating of a "neutral" node is 0.0. Pathrater doesn't modify the node rating if it is not in active use.

Watch dog and pathrater can increase network throughput by 27% during extreme mobility and at the same time increases percentage of transmission overhead from 12% to 24%.

E. Risk Awareness to MANET routing attack

A risk aware response mechanism is provided which will detect the intrusion and alert the nodes about malicious node. The usual existing systems will identify this intrusion and will isolate the victim node from the network. This can bring many irregularities in the network topology and communication between the nodes. The proactive routing protocol OLSR [8] is used. The major task of any routing protocol is to discover the network topology. OLSR protocol obtain route by periodic exchange of topology information between the nodes.



` Fig.4 Malicious Node Behaviour

From Fig.4 When a node 1 is being identified as the malicious node the isolation of the node from the network will partition the network, thus by making nodes 6 and node 7 disconnected. The proposed system does not isolate the node but evaluates the node behaviour based on the threshold set and decides whether it has to completely isolate or temporarily

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 11, November 2013

isolated.

The evidence collection and combination for deciding the node behaviour is based on extended Dempster Shafer theory [6] which is a theory of evidence and probable reasoning.

The risk aware response mechanism is divided into the following four steps. [7]

1. Evidence collection: In this step, Intrusion Detection System (IDS) gives an attack alert with a confidence value, and then Routing Table Change Detector (RTCD) runs to figure out how many changes on routing table are caused by the attack.

2. Risk assessment: Alert confidence from IDS and the routing table changing information would be further considered as independent evidences for risk calculation and combined with the extended D-S theory. Risk of countermeasures is calculated as well during a risk assessment phase. Based on the risk of attacks and the risk of countermeasures, the entire risk of an attack could be figured out.

3. Decision making: The adaptive decision module provides a flexible response decision-making mechanism, which takes risk estimation and risk tolerance into account. To adjust temporary isolation level, a user can set different thresholds to fulfil her goal.

4. Intrusion response: With the output from risk assessment and decision-making module, the corresponding response actions, including routing table recovery and node isolation, are carried out to mitigate attack damages in a distributed manner.

An adaptive decision making system [9] has been implemented in Fig.5. The response level is additionally divided into multiple bands. Each band is associated with an isolation degree, which presents a different time period of the isolation action. The response action and band boundaries are all determined in accordance with risk tolerance and can be changed when risk tolerance threshold changes. The upper risk tolerance threshold (UT) would be associated with permanent isolation response. The lower risk tolerance threshold (LT) would remain each node intact. The band between the upper tolerance threshold and lower tolerance threshold is associated with the temporary isolation response, in which the isolation time (T) changes dynamically based on the different response level given.

It implies when the risk of attack is greater than the risk of isolation response, the isolation is needed. If other information is available, it could be used to adjust thresholds.

For example, node reputation is one of important factors in MANET security; the adaptive decision-making module could take this factor into account as well. That is, if the compromised node has a high or low reputation level, the response module can intuitively adjust the risk tolerance thresholds accordingly.

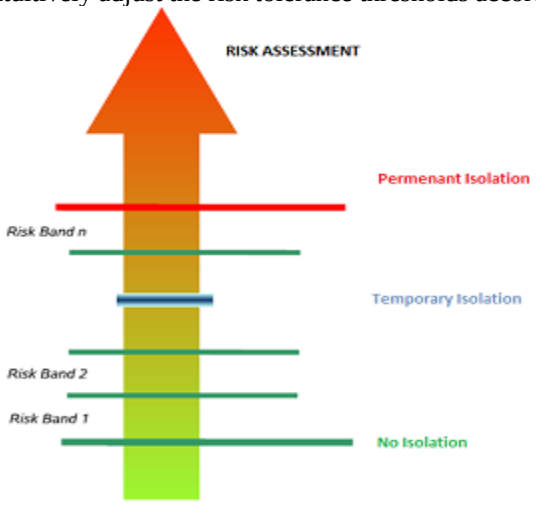


Fig.5. Adaptive Decision Making

III. Comparison Of Different Approach

Several works addressed the intrusion response actions [1], [2] in MANET by isolating uncooperative nodes based on the node reputation derived from their behaviours. In MANET scenario, improper countermeasures may cause the unexpected network partition, bringing additional damages to the network infrastructure.

To address the above-mentioned critical issues, more flexible and adaptive response should be investigated [7].

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 11, November 2013

TABLE I
COMPARISON OF EXISTING TECHNIQUES

Approach	Merits	Demerits
Trust Modelling and Evaluation	The trust worthiness of nodes are evaluated secure routing	Traffic overhead due to TRR
Reputation Management of nodes	Behaviour of nodes are evaluated	Approach was only based on selfish nodes
ADRS	Anomalous events are diagnosed Both in accidental errors and intentional attacks	Selfish nodes refuse to run IDS
Watchdog and Pathrater	Increase throughput	Transmission Overhead
Risk awareness to MANET routing attacks	Reduces Network partitioning due to isolation of malicious nodes	Packet overhead and byte overhead

Here above Table I give a comparison on the existing techniques.

IV. CONCLUSION

MANET is distinguished from other networks by virtue of its self configuring and optimizing nature. Due to its flexible nature, MANET is exposed to various attacks especially routing attacks. Various techniques are given to mitigate such critical attacks such as Intrusion Detection techniques. Intrusion detection system monitors and analyses the activities of the nodes and determines the performance with the security rules. It also alerts the neighbouring nodes if irregularity has been detected in the performance of a node. An intrusion Response System recovers the affected services and reconfigures the system. As topology of MANET changes continuously achieving security in these networks is very difficult.

Several techniques have been proposed for better performance of MANET. In MANET scenario, improper countermeasures may cause the unexpected network partition, resulting in added damage to the network infrastructure. To address these crucial issues, more open and adaptive response should be inspected. At present, the focus of MANET is towards mesh networking and large scale. Improvement in various areas such as security and bandwidth is required.

REFERENCES

[1] Y. Sun, W. Yu, Z. Han and K. Liu, "Information Theoretic Framework of Trust Modelling and Evaluation for Ad Hoc Networks," IEEE J. Selected Areas in Comm., vol. 24, no. 2, pp.305-317, Feb. 2006.

[2] M. Refaei, L. DaSilva, M. Eltoweissy, and T. Nadeem, "Adaptation of Reputation Management Systems to Dynamic Network Conditions in Ad Hoc Networks," IEEE Trans. Computers, vol. 59, no. 5, pp. 707-719, May 2010.

[3] A. Wald, Sequential Analysis. J. Wiley & Sons, 1947.

[4] S.Wang, C.Tseng, K. Levitt, and M. Bishop, "Cost-Sensitive Intrusion Responses for Mobile Ad Hoc Networks," Proc. 10th Int'l Symp. Recent Advances in Intrusion Detection (RAID '07), pp. 127-145, 2007.

[5] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating Routing Mis behaviour in Mobile Ad Hoc Networks," Proc. ACM MobiCom, pp. 255-265, 2000.

[6] G. Shafer, A Mathematical Theory of Evidence. Princeton Univ., 1976.

[7] Ziming Zhao, Hongxin Hu, Gail-Joon Ahn,and Ruoyu Wu "Risk-Aware Mitigation for MANET Routing Attacks" IEEE Transactions On Dependable And Secure Computing, vol. 9, no. 2, March/April 2012

[8] T. Clausen and P. Jacquet, "Optimized Link State Routing Protocol," Network Working Group, 2003.

[9] P. Cheng, P. Rohatgi, C. Keser, P. Karger, G. Wagner, and A.Reninger, "Fuzzy Multi-Level Security: An Experiment on Quantified Risk-Adaptive Access Control," Proc. 28th IEEE Symp. Security and Privacy, 2007.

[10] N. Mohammed, H. Otrok, L. Wang, M. Debbabi, and P. Bhattacharya, "Mechanism Design-Based Secure Leader Election
Model for Intrusion Detection in MANET,"IEEE Trans. Dependable and Secure Computing, vol. 8, no. 1, pp. 89-103, Jan./Feb. 2011.

[11] C. Strasburg, N. Stakhanova, S. Basu, and J. Wong, "Intrusion Response Cost Assessment Methodology, "Proc. Fourth ACM
Symp. Information, Computer, and Comm. Security (ASIACCS '09), pp. 388-391, 2009.

[12] Y. Hu, A. Perrig, and D. Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks," Proc. IEEE INFOCOM,vol. 3, pp. 1976-1986, 2004.

[13] D. Johnson, D. Maltz, Y.-C. Hu, and J. Jetcheva. The dynamic source routing protocol for mobile ad hoc networks.IEEE Internet Draft, March 2001. draft-ietf-manet-dsr-05.txt (work in progress).

BIOGRAPHY

Yamini.T is currently pursuing M.Tech in CSE at PVP Siddhartha Institute of Technology, Vijayawada, A.P, India. She has received her B.Tech degree in Computer Science & Information Technology from VIGNAN'S Engineering College, Guntur. Her main research interest includes Networking and Wireless Technology.

A.Sudhir Babu is currently working as Associate Professor in CSE department at PVP Siddhartha Institute of Technology, Vijayawada, A.P., India. He is having 20 years of experience in teaching. He Received Post Graduation M.Tech from the stream of Computer Science Engineering. His main research interest includes Networking and Wireless Sensor Networks.