IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 2, Ver. I (Mar-Apr. 2014), PP 26-31
www.iosrjournals.org

Survey on Intrusion Detection System in Heterogeneous WSN Using Multipath Routing

G.Saravanan[1], Pravin R.Patil[2], M.Rajeev Kumar[2#]

[1]M Tech Scholars, Dept. of Information Technology Vel Tech Dr.RR & Dr.SR Technical University, Chennai
[2#]Assistant Professor, Dept. of Information Technology Vel Tech Dr.RR & Dr.SR Technical University, Chennai
[2]Assistant Professor, Dept. of Computer Science and Engineering Pune Institute of Computer technology, Pune

Abstract: *In this paper, we propose an survey on heterogeneous wireless sensor network (HWSN) and how the efficiency and redundancy management is exploit in the various methods .Here timeliness and security are main concern to maximize the system lifetime by ensuring various methods like Intrusion detection system (ids), multipath routing, etc, The main goal of the paper is to reveal various methods which are used to maintain best redundancy level and increasing the energy efficiency.*

I. Introduction:

Wireless sensors networks (WSN) are planned in unattended surroundings in which energy replacement is difficult if not possible. Due to partial income, a WSN should not only assure the application specific QoS requirements such as timeliness, security, and reliability, but also reduce energy consumption to extend the system helpful lifetime. The WSN aim is maximize the system lifetime exchange between the energy consumption vs. reliability. However, no previous work exists to consider the exchange in the presence of malicious attackers. It is commonly believed in the explore neighborhood that cluster is an effective solution for reach scalability, energy conservation, and reliability. If use homogeneous nodes which rotate among themselves in the roles of cluster heads (CHs) and sensor nodes (SNs) leveraging CH election protocols such as HEED [10] for lifetime maximization has been consider. Demonstrated that using heterogeneous nodes can further improve performance and extend the system lifetime. In the last case, nodes with greater resources provide as CHs performing computation all intensive tasks while inexpensive less capable SNs are utilized mainly for sensing the environment. The tradeoff issue between energy consumption vs. QoS increase becomes much more difficult when inside attackers are present as a path may be broken when a malicious node in the path. The case in heterogeneous Wireless Sensor Network (HWSN) environments in which CH nodes may take a more critical role in gathering and routing intellect data. The system would occupy an intrusion detection system (IDS) with the purpose to detect and remove the malicious node. While the literature is plentiful in intrusion detection techniques for WSNs [3], the issue of how often intrusion detection should be invoked for energy reasons in order to remove potentially malicious nodes so that the system lifetime is maximized are largely unfamiliar. The issue is particularly dangerous for energy constrained WSNs designed to stay alive for a long mission time. The multipath routing is regard as an efficient mechanism designed for fault and intrusion tolerance to get better data release 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. The most previous research focused on using multipath routing to improve reliability [3], some attention has been paid to using multipath routing to tolerate inside attacks. These studies, still, mainly unobserved the exchange between QoS gain vs. energy consumption which can harmfully shorten the system lifetime. The research problem we are addressing in this paper is efficient redundancy management of a clustered HWSN to extend its lifetime process in the presence of unreliable and malicious nodes. We address the exchange between energy consumption vs. QoS gain in as timeliness, security, and reliability through the goal to exploit the lifetime of a clustered HWSN as fulfilling application QoS requirements in the environment of multipath routing. We study the best amount of redundancy through which data are routed to a remote sink in the presence of unreliable and malicious nodes, so query success probability is exploiting while maximizing the HWSN lifetime. This optimization problem designed for the case in which a voting based distributed intrusion detection algorithm is used to eliminate malicious nodes from the Heterogeneous Wireless sensor network (HWSN). Our contribution is a model-based analysis methodology by which the optimal multipath redundancy levels and intrusion detection settings may be identified for satisfying application QoS requirements while maximizing the lifetime of HWSNs. For the issue of intrusion tolerance through multipath routing, there are two major problems to solve one is how many paths to use and second one is what path to use. To the finest of our information, we are the first to address the “how many path to use” problem designed for the “what path to use” problem, our evolution on the before than is different from presented effort in that we do not consider specific routing protocols, nor the use of feedback information to explain the trouble. Somewhat, for energy conservation, we use a distributed light-weight IDS by which intrusion detection is performed only local. Nodes that are identified compromised are removed from the HWSN. Only compromise nodes that live on detection have the chance to concern routing. One main contribution of our paper is that we decide "how many paths to use" in order to tolerate residual compromised nodes that live on our IDS, so as to maximize the HWSN lifetime.

II. Previous Works:

A three-layered architecture [1] was proposed for randomly deployed heterogeneous wireless sensor networks. An additional algorithm for relay node selection also was presented. Lastly, simulation has been done to demonstrate the effectiveness of the proposed algorithm to improve the network lifetime.

A wireless sensor network [2] consists of a group of embedded devices called sensor nodes reading, computing and reporting data to the local coverage area. The applications of wireless sensor networks are promising to make our lives added suitable. One of the vast issues facing sensor node is the energy constraint due to only having a small battery as their energy. Efficiency of energy consumption and prolonging network lifetime are challenge. This survey paper aims to collect and classify contemporary approaches of effective energy consumption in wireless sensor networks.

A survey of Intrusion Detection Systems (IDSs) [3] that are proposed for WSN is offered. First one is detailed information about IDSs is present. Second one is a brief survey of IDSs proposed for Mobile Ad-Hoc Networks (MANETs) is presented and applicability of those systems to WSN is discussed. Third one is, IDSs planned for WSN are offered. This is followed by the analysis and comparison of each scheme along with their advantages and disadvantage. Lastly, plan on IDSs that are potentially applicable to WSNs are provided

We extend adaptive fault-tolerant quality of service (QoS) [4]organize algorithms support on hop-by-hop data delivery utilize "source" and "path" redundancy, by the plan to suit application QoS requirements while widen the lifetime of the sensor system. We enlarge a mathematical model for the lifetime of the sensor system as a function of system limit including the "source" and "path" redundancy levels utilized. We find out that there be present best "source" and "path" redundancy under which the lifetime of the system is maximized while fulfilling application QoS requirement. Numerical information is real and confirm through wide simulation, with physical explanation given, to tell the feasibility of our algorithm design.

We investigates the usefulness of multi-path routing [5] to achieve lifetime improvements by load balancing and exploiting cross-layer information in wireless sensor networks. Presentation increase in the order of 10-15 % could be achieved by altering path update rules of existing on-demand routing method. Problems meet with parallel traffic along interfering paths have been identified as a direct consequence of special MAC protocol properties.

We consider [6] the cluster-based heterogeneous wireless sensor network, they are two different types of nodes, namely, the powerful cluster-heads and the inexpensive sensor nodes. In particular, in the WSN, the sensor nodes are deployed along the grid points. To better balance the energy consumption, the sensor nodes exchange data with the cluster-heads through mixed communication modes, i.e., they can communicate with cluster heads by either single-hop or multi-hop mode. Given the initial energy of the sensor nodes, we develop the analytical models to derive the optimal communication range and identify the optimal mixed communication modes to maximize the span of WSN's lifetime. Also presented are the simulation results which verify our developed analytical models.

We here a new packet release mechanism called Multi-Path and Multi Speed Routing Protocol (MMSPEED) [7], in favor of probabilistic Quality of Service (QoS) security in wireless sensor networks. The Quality of Service (QoS) provisioning is carrying out in two quality area namely reliability and timeliness. Multiple QoS stages are provided in the timeliness domain by assurance multiple packet release speed opportunity. In the consistency area, various reliability requirements are supported by probability multipath forward. This mechanism designed for QoS provisioning are take in a localized way exclusive of universal network information by employing localized geographic packet forwarding improved with dynamic reward, which recompense for incomplete end incorrectness as a packet movements towards its target. This method, MMSPEED can promise end-to-end requirements in a restricted method, which is smart for adaptability and scalability to great scale dynamic sensor network. Simulation result explain that MMSPEED offer QoS differentiation in both reliability and timeliness domains and, as an result, a lot improves the efficient ability of a sensor network in conditions of number of run that meet both timeliness and reliability supplies up to fifty percent

We calculate [8] the shock of number and placement of heterogeneous resources on performance in networks of unlike volume and density. We explain that best use is very hard in general; we also explain that only a modest number of reliable, line-powered nodes and long-range backhaul links are required to have an important impact. Properly arrange, heterogeneity be able to triple the regular delivery rate and supply a 5-fold boost in the lifetime of a great battery-powered network of easy sensors.

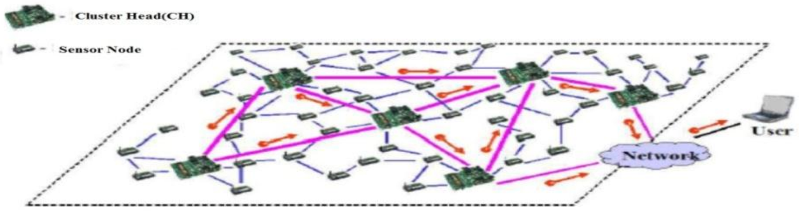
We propose [9] a distributed, randomized clustering algorithm to organize the sensors in a wireless sensor network into clusters. We after that extend this algorithm to make a hierarchy of cluster heads and observe that the energy savings increase with the number of levels in the hierarchy. Outcome in stochastic geometry are used to derive solutions for the values of parameters of our algorithm that minimize the total energy spent in the network when all sensors report data through the cluster heads to the processing center.

We propose [10] a novel distributed clustering approach for long-lived ad hoc sensor networks. Our future move toward does not make any assumptions about the presence of infrastructure or about node ability, other than the availability of multiple power levels in sensor nodes. We present a protocol, HEED (Hybrid Energy-Efficient Distributed clustering), that periodically selects cluster heads according to a hybrid of the node residual energy and a minor limit, such as node proximity to its neighbors or node level. HEED terminates in iterations, incurs low message overhead, and achieves fairly uniform cluster head distribution crossways the network. We establish that, with appropriate bounds on node density and intra cluster and inter cluster transmission ranges; HEED can asymptotically almost surely guarantee connectivity of cluster network. Simulation results show that our proposed approach is effective in prolonging the network lifetime and supporting scalable data aggregation.

We explain an Intrusion-tolerant routing protocol for wireless Sensor Networks (INSENS) [11]. INSENS make onward tables at each node to make easy communication between sensor nodes and a base station. It ease working out, storage, bandwidth and communication requirements at the sensor nodes at the cost of better computation, storage, bandwidth and communication requirements at the base station. INSENS is not rely on recognize intrusions, other than slightly tolerates intrusions by sidestep the malicious nodes. A very important possession of INSENS is that while a malicious node may be able to cooperation a small number of nodes in its region, it cannot reason extensive damage in the network.

III. Heterogeneous Wireless Sensor Network:

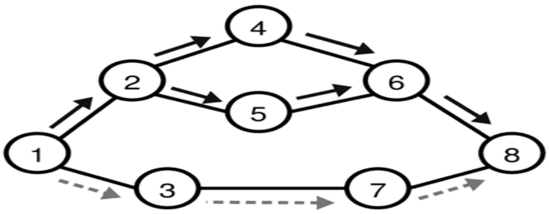
The [9] heterogeneous model in a heterogeneous wireless sensor networks (HWSNs) is different from that in heterogeneous wireless networks. In HWSNs, the heterogeneous model refers to the characteristics of the sensor node itself: it has more energy, more bandwidth capability, or more processing capability. The concept of the heterogeneous wireless sensor networks (HWSNs). The network consists of two types of nodes, i.e., the sensor nodes and Cluster Head (CH), with different energy capabilities. The figure shows that the Cluster Head (CH) collect data from all the sensor nodes and send them to the user. This process continues until the battery energy is drained.



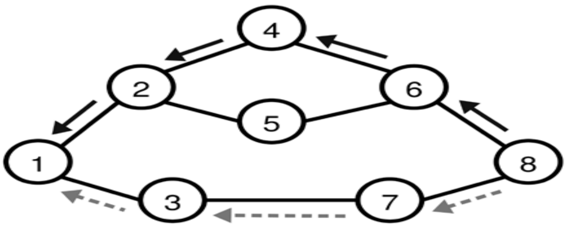
Architecture of a heterogeneous wireless sensor networks

IV. Multipath Routing Protocol:

Several [5] multi-path protocols for wireless ad-hoc networks such as the Ad-hoc On Demand Distance Vector Multi-path routing protocol (AODVM) which is an extension of AODV for discovering node-disjoint or optionally link-disjoint paths It finds node-disjoint paths by exploiting a particular property of flooding. To find node-disjoint routes, nodes do not immediately reject Route Request. Each Route Request arriving via a different neighbor of the source has a different first-hop in the Route Request header, and therefore defines a node-disjoint path.



Route Request



Route Reply

Table 1. Routing table node#1

Dest	Next	Hops	Seq
8	3	3	37
8	2	4	37

Table 2.Routing table node#6

Dest	Next	Hops	Seq
1	4	3	11
8	8	1	37

The destination node only answers to the first incoming RREQ with a corresponding RREP from neighbor9. The duplicate RREQ from neighbor 11 is simply discarded and left unanswered, as it advertises the same sequence number with our approach, only the hop-count optimal routes via nodes 9 and 11.

4.1. Benefits of Multi-Path Routing:

It is mainly intended to discover one single route from a source to a destination. All through the route discovery method, these protocols aim to find the best route with the lowly cost. Multi-path routing protocols aim to find multiple routes. Multi-path routing has been investigated in the Internet, in municipal and local area networks , as well as in wireless sensor networks find out and maintaining multiple paths causes certain transparency, but yields several advantages, namely load balancing, bandwidth aggregation ,fault tolerance, reduced delay

4.1.1. Load Balancing:

Multi-path routing can avoid congestion and improve performance. In wireless sensor networks, the main focus of multi-path routing is typically on the load balancing issue .As nodes are constraint to a limited amount of energy, and traffic is likely to be low, the key worry is to keep the network operable for a maximum total of time, In sensor networks, one has to deal with traffic generated by many leaf nodes attempting to deliver data to one or a few sinks. It has been observed that in such cases nodes that have to forward traffic from large sub-trees suffer much earlier from energy depletion, when nodes collaborate in sensing and data forwarding and packets are not always routed on the same routes, but the load is balanced over multiple routes, network lifetime can be increased significantly

4.1.2. Bandwidth Aggregation:

By splitting data to the same destination into multiple streams, each stream is routed through a different path. This strategy is especially beneficial when a node has multiple low bandwidth links but requires higher bandwidth than each individual link can provided

4.1.3. Fault Tolerance:

Multi-path routing protocols can increase the degree of fault tolerance by having redundant information routed to the destination in excess of exchange paths. This boost the energy transparency, but helps to reduce the probability that communication is disrupted and data is lost in case of link failures the trade-off between the additional overhead and the reliability gain has been investigated.

4.1.4. Reduced Delay:

In wireless networks running single path on-demand routing protocols, route failures trigger the path discovery process to find new routes causing route discovery delay. Delay can be reduced in multi-path routing, as backup routes can be identified immediately, Quality-of-Service (QoS) characteristics of both paths permits to switch the load to another route whenever the service parameters of another route promise better quality

4.1.5. Route Coupling:

As nodes in the network correspond through the wireless standard, radio intrusion must be taken into description. Transmissions along one path may interfere with transmissions along another path, even if the paths are link-disjoint or even node-disjoint. Route coupling occurs when two routes are located physically close enough to interfere with each other during transmission. The advantages of two routes being available are therefore limited.

V. Intrusion Detection Systems (Ids):

In [3] a network or a system, any kind of unauthorized or unapproved activities are called intrusions. An Intrusion Detection System (IDS) is a collection of the tools, technique, and assets to help identify, assess, and statement intrusions. Intrusion detection is normally one part of an overall protection system that is installed around a system or device and it is not a stand-alone protection measure. In intrusion is defined as: “any set of actions that attempt to compromise the truthfulness, confidentiality, or availability of a resource” and intrusion prevention techniques2 are presented as the first line of defense against intrusions. However, as in any kind of security system, intrusions cannot be totally prevented. The intrusion and compromise of a node leads to confidential information such as security keys being revealed to the intruders. This results in the failure of the preventive security mechanism. Therefore, IDSs are designed to make public intrusions, before they can disclose the secured system resources. IDSs are always considered as a second wall of defense from the security point of view. IDSs are cyberspace equivalent of the burglar alarms that are being used in physical security systems today. As mentioned in,

The expected operational requirement of IDSs is given as: “low false positive rate, calculated as the percentage of normalcy variations detected as anomalies, and high true positive rate, calculated as the percentage of anomalies detected”.

5.1. Requirements of IDS:

The IDS that is being designed should satisfy the following requirements

- Not introduce new fault to the system.
- require little system resources and should not disgrace overall system performance by introducing overheads.
- run constantly and remain transparent to the system and the users.
- used in normal to be cooperative and open.
- be reliable and reduce false positives and false negatives in the detection phase.

5.2. Classification of IDS:

1) Intruder type: Intruders to a network can be classified into two types:

- External intruder: An outsider using different means of attacks to reach the network.
- Internal intruder: A compromised node that used to be a member of the network. according to insider attacks against ad-hoc networks use two types of nodes:
  - – Selfish node: Uses the network resources but doesn’t help, save battery life for their own communications. It does not directly injure other nodes.
  - – Malicious node: Aims at injure other nodes by causing network DoS by partitioning, while saving battery life is not a priority.

IDS can detect both external and internal intruders, but it should be noted that internal intruders are harder to detect. This is due to the fact that internal intruders have the necessary key materials to neutralize any precautions taken by the authentication mechanisms.

2) Intrusion type: Intrusions in a network may happen in various ways:

- Attempted break-in: An attempt to have an unauthorized access to the network.
- Masquerade: An attacker uses a fake identity to gain unauthorized access to the network.
- Penetration: The acquisition of unauthorized access to the network.
- Leakage: An undesirable information flow from the network.
- DoS: Blockage of the network resources to the other users.
- Malicious use: Deliberately harming the network resources.

IDSs may provide partial detection solution to those attacks. But of course, all system administrators would like to have perfect IDS that would able to detect all of the intrusions listed above

.

5.3. Challenge of IDS:

The unique characteristics of sensor nodes pose challenges to the construction of a WSN IDS. AWSN has a limited power supply, energy-efficient protocols and applications to maximize the lifetime of sensor networks Sensor nodes are prone to failure Also, a WSN usually is densely deployed, causing serious radio channel contention and scalability problems. The design of an effective WSN IDS must bear in mind all of these challenge

5.3.1. Secure Localization in WSN

Therefore, many localization protocols have been proposed to help sensor nodes to estimate their locations To utilize localization protocols, some special nodes, called beacon nodes These beacon nodes are assumed to know their locations and transmit their locations to other non-beacon nodes through beacon packets. Non-beacon nodes also estimate certain measurements. Localization protocols may become vulnerable when a WSN is deployed in a hostile environment that each non-beacon node can efficiently detect location anomalies by verifying whether estimated locations if the level of inconsistency is above a predefined threshold, sensor nodes can decide that received location references are malicious. If the mean square error is larger than a threshold, non-beacon nodes could think that the received set of location references is malicious. The second approach is the voting-based location estimation The non-beacon node can then have every received location reference vote on the cells in which this node may reside and thus decide how likely this node is in each cell. After the voting process, the center of the cells with the highest votes may be used as the estimated location.

5.3.2. Secure Aggregation in WSN:

Aggregation has become one of the required operations for a WSN to save energy introduces a theoretical framework to model and to analyze the resilient data aggregation problem propose a Secure Hop-by-Hop Data Aggregation Protocol (SDAP) for WSNs The design of SDAP is based on divide-and-conquer and commit-and-attest principles a hop-by-hop aggregation is make and one total is generated from a group. This hop-by-hop aggregation is enhanced to ensure that each group cannot deny its committed aggregate.

VI. Clustering Due To Energy Consumption:

For clustering the system would consume energy for broadcasting the announcement message and for the Cluster join process [5]. Since p is the probability of becoming a CH, there will be pn SNs that would be broadcasting the statement message. This statement message will be received and retransmitted by each SN to the next hop until the TTL of the message reaches the value the number of hops equals. [9]Thus, the energy required for broadcasting. The cluster-join process will require an SN to send a message to the CH informing that it will join the cluster and the CH to send an acknowledgement to the SN. Since there are pn CHs and SNs in the system, the energy for this islet the size of the message exchange is NL.ER and ET will be calculated from (1) and (2) with NL in place of nb. Let be the number of iterations required to implement the clustering algorithm. Then, the energy required for each implementation of the clustering algorithm.

VII. Conclusions:

In this paper, we surveyed various methods to find out the best redundancy level and multipath routing which is necessary to increase the energy consumption by provides best redundancy path. Here timeliness QOS in reliability, security are main concern while using these methods.

References:

[1] Norah Tuah and Mahamod Ismail “Extending Lifetime of Heterogeneous Wireless Sensor Network using Relay Node Selection” International Conference of Information and Communication Technology (ICoICT), 2013

[2] Anuparp Boonsongsrikul, Slavko Kocijancic and Somjet Suppharangsan “Effective Energy Consumption on Wireless Sensor Networks: Survey and Challenges” MIPRO 2013, May 20-24, 2013

[3] Ismail Butun, Salvatore D. Morgera, and Ravi Sankar “A Survey of Intrusion Detection Systems in Wireless Sensor Networks” IEEE COMMUNICATIONS SURVEY, Issue: 99, 2013

[4] Ing Ray Chen, Anh Phan Speer, Mohamed Eltoweissy “Adaptive Fault Tolerant QoS Control Algorithms for Maximizing System Lifetime of Query Based Wireless Sensor Networks” IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 8, NO. 2, MARCH-APRIL 2011

[5] Philipp Hurni and Torsten Braun “Energy-Efficient Multi-Path Routing in Wireless Sensor Networks” 7th International Conference, September 10-12, 2008

[6] Hang Su and Xi Zhang “Network Lifetime Optimization for Heterogeneous Sensor Networks with Mixed Communication Modes” IEEE Communications Society subject matter experts for publication in the WCNC 2007

[7] Emad Felemban, Chang-Gun Lee, Eylem Ekici “MMSPEED: Multipath Multi-SPEED Protocol for QoS Guarantee of Reliability and Timeliness in Wireless Sensor Networks” IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 5, NO. 6, JUNE 2006

[8] Mark Yawis, Nandakishore Kushalnagar, Harkirat Singh, Anand Rangarajan, York Liu, Suresh Singh “Exploiting Heterogeneity in Sensor Networks”INFOCOM 2005,24th Annual Joint Conference of the IEEE Computer and Communications Societies. IEEE, 2005

[9] Seema Bandyopadhyay and Edward J Coyle “An Energy Efficient Hierarchical Clustering Algorithm for Wireless Sensor Networks” INFOCOM 2005, 24th Annual Joint Conference of the IEEE Computer and Communications Societies, 2005

[10] Ossama Younis, Sonia Fahmy, “HEED: A Hybrid, Energy-Efficient, Distributed Clustering Approach for Ad Hoc Sensor Networks” IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 3, NO. 4, OCTOBER-DECEMBER 2004

[11] Jing Deng, Richard Han, Shivakant Mishra “INSENS: Intrusion-Tolerant Routing in Wireless Sensor Networks” University of Colorado, Department of Computer Science Technical Report CU-CS-939-02