Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 8, August 2014, pg.162 – 169

RESEARCH ARTICLE

Idleness Scheming and Intrusion Tolerance using Acknowledgement through Multipath Routing in Heterogeneous Wireless Sensor Network

Sachin Singh V. Thakur*, Prof. Rachana Kambale, Kshama Dwivedi*****

*Pursuing Masters of Technology in Computer Science from T.I.T. Bhopal (M.P., India)
**Assistant Professor Department of Computer Science and Engineering, T.I.T. Bhopal (M.P., India)
*** Pursuing Masters of Engineering Department of Computer Science and Engineering, ARIET, Mumbai (M.H., India)
* mr.svthakur@gmail.com
** rachanakamble@gmail.com
*** kshama1410@gmail.com

Abstract- In this research, we propose the controlling of duplication of Components or data to provide survival of the total system in case of failure of single component in HWSN, by using dynamic multipath routing to send data to sink(base station) in the presence of unreliable and malicious nodes. Normally for transmission the path is formed while initialization of network like in case of TCP/IP protocol. The research that we are formulating focuses on redundancy controlling to exploit the tradeoff between energy consumption vs the gain in reliability, timeliness by dynamic multipath routing to maximize the system useful lifetime. For these reasons, we formulate the acknowledgement system in between nodes, cluster heads, processing center and sink. When cluster heads sends data to the processing center and then to sink at that time sink will keep that path as reliable path in its logs and again sends acknowledgement to the senders end and considers this path as reliable for further transmission. What it yields is the reliability, security, timeliness. If this acknowledgement is not available in HWSN then the data will be sent repeatedly to malicious cluster by the sender if any present in the network. Thus it will consume more energy because of repeated transmission. So acknowledgement avoids this repeated transmission which results in conservation of energy by detecting and evicting malicious node in HWSN. Furthermore, we consider this optimization problem for the case in which voting based distributed intrusion detection algorithm is applied. We then apply the logs obtained at base station to design dynamic redundancy controlling algorithm to formulate and implement the best design parameters settings at runtime in response to environmental changes to maximize HWSN lifetime.

Keywords— Idleness Scheming, Energy Conservation, Heterogeneous Wireless Sensor Network, Intrusion Tolerance with Acknowledgement, Multipath Routing, Reliability, Timeliness, Security

I. INTRODUCTION

ensor Network is consist of various sensor nodes which are used for different purposes like in research areas, military, medical science and aeronautical engineering etc. for capturing or fetching important and meaningful data for the future used. There are various types of attacks on sensor networks. Although, intrusion prevention measures such as strong authentication and redundant transmission can be used to improve the security of these networks, these techniques can address only a subset of the threats and they are very costly to implement. Each node has only less number of resources, because of this it is difficult to achieve QoS requirements such as reliability timeliness, security and minimize energy consumption to increase the system lifetime. The scalability, reliability and energy conservation can be achieved using clustering. For data delivery as well as fault tolerance and intrusion detection purpose in Heterogeneous Wireless Sensor Network multipath routing mechanism is very effective. Network parameters such as sensing range, node density and transmission range have to be carefully considered according to specific applications, at the network design stage. In order to achieve this, it is essential to capture the impacts of network parameters on network performance with respect to application specification. Intrusion Detection System is capable to finding the malicious nodes and handling them for energy conservation mechanism to increase system lifetime [5], [9].

A wireless network is any type of computer network that uses wireless data connections for connecting network nodes. Wireless networking is a method by which homes, telecommunications networks and enterprise (business) installations avoid the costly process of introducing cables into a building, or as a connection between various equipment locations. Wireless telecommunications networks are generally implemented and administered using radio communication. The intrusion detection can be analyzed according to the capability of sensors in terms of the transmission range and sensing range. In a heterogeneous WSN some sensors have a large power to achieve a longer transmission range and large sensing range. Recent studies [2], [3] demonstrated that using heterogeneous nodes can enhance performance and prolong the system lifetime [12], [13]. In the latter case, nodes with superior resources serve as CHs performing computationally intensive tasks while inexpensive less capable SNs are utilized mainly for sensing the environment. Thus, the heterogeneous WSN increases the detection probability for a given intrusion detection system. It is commonly believed in the research community that clustering [4], is an effective solution for achieving scalability, energy conservation, and reliability. Therefore the cluster based heterogeneous WSN can further improves the Figure performance of the network. Cluster-based Wireless Sensor Network (CWSN) is shown.

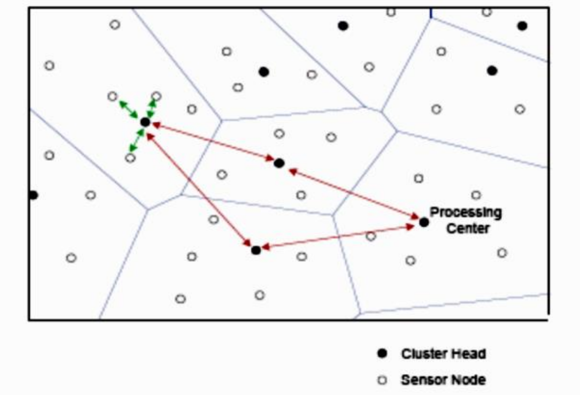

Fig 1: Cluster based Heterogenous Wireless Sensor Network.

Heterogeneous Wireless LAN

A wireless local area network (WLAN) links two or more devices over a short distance using a wireless distribution method, usually providing a connection through an access point for Internet access. The use of spread-spectrum technologies may allow users to move around within a local coverage area, and still remain connected to the network. Fixed technology implements point-to-point links between computers or networks at two distant locations, often using dedicated microwave or modulated laser light beams over line of sight paths. A computer cluster consists of a set of loosely connected or tightly connected computers that work together so that in many respects they can be viewed as a single system [6]. The components of a cluster are usually connected to each other through fast local area networks ("LAN"), with each *node* (computer used as a server) running its own instance of an operating system. Computer clusters emerged as a result of convergence of a number of computing trends including the availability of low cost microprocessors, high speed networks, and software for high performance distributed computing [10]. A heterogeneous network is a network connecting computers and other devices with different operating systems and/or protocols. For example, local area networks (LANs) that connect Microsoft Windows and Linux based personal computers are heterogeneous. The word heterogeneous network is also used in wireless networks using different access technologies [7]. For example, a wireless network which provides a service through a wireless LAN and is able to maintain the service when switching to a cellular network is called a wireless heterogeneous network. A wireless mesh network is a wireless network made up of radio nodes organized in a mesh topology. Each node forwards messages on behalf of the other nodes. Mesh networks can "selfheal", automatically re-routing around a node that has lost power. Wireless metropolitan area networks are a type of wireless network that connects several wireless LANs. WiMAX is a type of Wireless MAN and is described by the IEEE 802.16 standard [1].

Semantic of “Heterogeneous Network” in Telecommunications

From a semantically point of view, it is very important to note that the Heterogeneous Network terminology may have different connotations in wireless telecommunications. For instance, it may refer to the paradigm of seamless and ubiquitous interoperability between various multi-coverage protocols. Otherwise, it may refer to the non-uniform spatial distribution of users or wireless nodes. Therefore, using the term "heterogeneous network" without putting it into perspective may result in a source of confusion in scientific literature and during the peer-review cycle. A wireless sensor network (WSN) of spatially distributed autonomous sensors to *monitor* physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling *control* of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on.

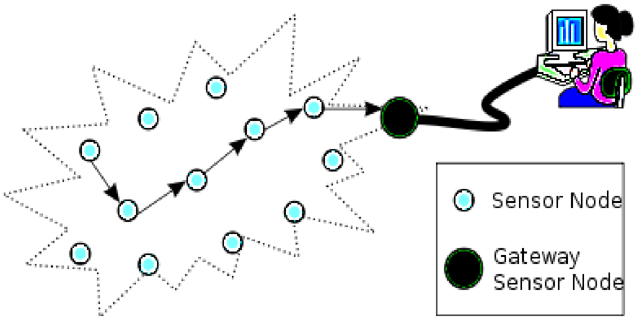

Fig: 2 typical multi-hop wireless sensor network architecture

The WSN is built of "nodes" – from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. Each such sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting. A sensor node might vary in size from that of a shoebox down to the size of a 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 a few to hundreds of dollars, depending on the complexity of the individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and communications bandwidth[8]. The topology of the WSNs can vary from a simple star network to an advanced multi-hop wireless mesh network. The propagation technique between the hops of the network can be routing or flooding. Cross-layer is becoming an important studying area for wireless communications. In addition, the traditional layered approach brings three main problems to us. First, traditional layered approach cannot share different information among different layers , which leads to each layer not having complete information. Second, the traditional layered approach cannot guarantee the optimization of the entire network. The traditional layered approach does not have the ability to adapt to the environmental change. Because of the interference between the different users, access confliction, fading, and the change of environment in the wireless sensor networks, traditional layered approach for wired networks is not applicable to wireless networks, third. So we can use cross-layer to make the optimal modulation to improve the transmission performance, such as data rate, energy efficiency, QoS (Quality of Service), etc. Sensor nodes can be imagined as small computers, extremely basic in terms of their interfaces and their components. They usually consist of a *processing unit* with limited computational power and limited memory, *sensors* or MEMS (including specific conditioning circuitry), a *communication device* (usually radio transceivers or alternatively optical), and a power source usually in the form of a battery. Other possible inclusions are energy harvesting modules,[8] secondary ASICs, and possibly secondary communication interface (e.g. RS-232 or USB).

The base stations are one or more components of the WSN with much more computational, energy and communication resources. They act as a gateway between sensor nodes and the end user as they typically forward data from the WSN on to a server. Other special components in routing based networks are routers, designed to compute, calculate and distribute the routing table. Network design is the first step in building a heterogeneous WSN with regular nodes and robust nodes that can withstand the harsh environmental conditions. We are interested in problems in which we have to design a heterogeneous network with multiple classes of nodes with different costs. This class of problems is important when we are presented with a network design budget for a heterogeneous network, where nodes of different classes have different efficiency of operation in diverse environments. Since WSNs comprise of nodes with non-replenish able batteries, it is crucial to design such a network with network lifetime in consideration. In the absence of a specified economic constraint on network design, one way to do this would be the deployment of dense heterogeneous networks, where redundancy can aid in prolonging network lifetime by rotation of nodes. However, most realistic design scenarios impose an economic constraint on network design and it is crucial to develop a framework where economic constraints are balanced with network sensing and lifetime objectives.

II. RELATED WORK

In Existing System, effective redundancy management of clustered HWSN to prolong its operation in the presence of unreliable and malicious nodes. We address the trade-off between energy consumption vs. QoS gain in reliability, timeliness and security with the goal to maximize lifetime of HWSN while satisfying application QoS requirement in context of multipath routing. OVER the last few years, we have seen a rapid increase in the number of applications for wireless sensor networks (WSNs). WSNs can be deployed in battlefield applications, and a variety of vehicle health management and condition-based maintenance applications on industrial, military, and space platforms. For military users, a primary focus has been area monitoring for security and applications. A WSN can be either source-driven or query-based Depending on the data flow. In source-driven WSNs, sensors initiate data transmission for observed events to interested users, including possibly reporting sensor readings periodically. An important research issue in source driven WSNs is to satisfy QoS requirements of event-to-sink data transport while conserving energy of WSNs. In query based WSNs, queries and data are forwarded to interested entities only. In query-based WSNs, a user would issue a query with QoS requirements in terms of reliability and timeliness.

Existing research efforts related to applying redundancy to satisfy QoS requirements in query-based WSNs fall into three categories: traditional end-to-end QoS, reliability assurance, and application-specific QoS. Traditional end-to-end QoS solutions are based on the concept of end-to-end QoS requirements. The problem is that it may not be feasible to implement end-to-end QoS in WSNs due to the complexity and high cost of the protocols for resource-constrained sensors. An example is Sequential Assignment Routing (SAR) that utilizes path redundancy from a source node to the sink node. Each sensor uses a SAR algorithm for path selection. It takes into account the energy and QoS factors on each path, and the priority level of a packet. For each packet routed through the network, a weighted QoS metric is computed as the product of the additive QoS metric and a weight coefficient associated with the priority level of that packet. The objective of the SAR algorithm is to minimize the average weighted QoS metric throughout the lifetime of the network. The algorithm does not consider the reliability issue.

III. PROPOSED WORK

In this paper we Propose Idleness Scheming and Intrusion Tolerance using Acknowledgement through Multipath Routing in Heterogeneous Wireless Sensor Network**.** We developed a novel probability model to analyses the best redundancy level in terms of path redundancy and source redundancy as well as the best intrusion detection systems in term of numbers of voters and intrusion invocation interval under which the life time of HWSN is maximized. We then apply the analyzed the results obtained to the design of dynamic redundancy management algorithm to identify and apply the best design parameter setting at run time in response to environment changes to maximize HWSN lifetime a three tier HWSN with objective of maximizing network lifetime while fulfilling power management and coverage objective Modules:

1) Multipath Routing
2) Intrusion Tolerance
3) Energy Efficient
4) Simulation Process

1. Multipath Routing: In this module, multipath routing is considered an effective mechanism for fault and intrusion tolerance to improve data delivery in HWSN. The basic idea is that the probability of at least one path reaching the sink node or base station increases as we have more paths doing data delivery. While most prior research focus on using multipath routing to improve reliability some attention has been paid to using multipath routing to tolerate insider attacks. These studies however, largely ignore the tradeoff between quality of service gain vs. energy consumption which can adversely shorten the system lifetime.
2. Intrusion tolerance: In this module, we are solving two major problems to the best of our knowledge, we are the first to address the “how many path to use “problem. For the “what paths to use “problem our approach is distinct from existing work. In that we do not consider specific routing protocols.”
3. Energy Consumption: In this module there are two approaches implemented. One approach especially applicable to flat HWSNs is for an intermediate node to feedback maliciousness and energy status of its neighbored nodes to the sender nodes (e.g. the source or sink nodes) who can then utilize the knowledge to rout packets to avoid nodes with unacceptable maliciousness or energy status. Another approach which we adopt in this paper is to use local host base IDS for energy conservation.
4. Simulation Process: In this module, the cost of executing dynamic redundancy algorithm management including periodic clustering, intrusion detection and query processing through multipath routing in terms of energy consumption.

IV. System Model

An Intrusion Detection System (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station. IDS come in a variety of “flavors” and approach the goal of detecting suspicious traffic in different ways. There are network based (NIDS) and host based (HIDS) intrusion detection systems. Some systems may attempt to stop an intrusion attempt but this is neither required nor expected of a monitoring system. Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible incidents, logging information about them, and reporting attempts. In addition, organizations use IDP systems for other purposes, such as identifying problems with security policies, documenting existing threats and deterring individuals from violating security policies. IDP systems have become a necessary addition to the security infrastructure of nearly every organization. IDP systems typically record information related to observed events notify security administrators of important observed events and produce reports. Many IDP systems can also respond to a detected threat by attempting to prevent it from succeeding. They use several response techniques, which involve the IDPS stopping the attack itself, changing the security environment (e.g. reconfiguring a firewall) or changing the attack's content [1]. .

V. Probability model

In this section we develop a probability model to estimate the Mean Time To Failure MTTF of a HWSN using multipath data forwarding to answer queries issued from a mobile user roaming in the HWSN area. The basic idea of our Mean Time to Failure (MTTF) formulation is that we first deduce the maximum number of queries, Nq, the system can possible handle before running into energy exhaustion for the best case in which all queries are processed successfully. Because the system evolves dynamically, the amount of energy spent per query also varies dynamically. Given the query arrival rate λ q as input, the average interval between query arrivals is 1/λq. So we can reasonably estimate the amount of energy spent due to query processing and intrusion detection for query j based on the query arrival time tQ,j. Next we derive the corresponding query success probability Rq (tQ,j), that is, the probability that the response to query j arriving at time tQ,j is delivered successfully to the PC before the query deadline expires. Finally, we compute MTTF as the probability-weighted average of the number of queries the system can handle without experiencing any deadline, transmission, or security failure. The MTTF is computed by,

$$\mathrm{MTTF}= \sum_{i=1}^{Nq-1} i\left(\prod_{i=1}^{i} Rq(t_{Q,J})\right)\ \ (1\text{-}R_q(t_{Q,I+1})) + \ N_q \prod_{j=1}^{N_q} R_q(t_{Q,j})$$

Algorithm for Dynamic Redundancy Management of Multipath Routing

```
CH Execution:
Get next event
If event is TD timer then
determine radio range to maintain CH connectivity
determine optimal TIDS,m,ms,mp by table lookup based on the current estimated density ,CH radio range and compromise rate
notify SNs within the cluster of the new optimal settings of TIDS and m
else if event is query arrival then
trigger multipath routing using ms and mp
else if event is T clustering timer then
perform clustering
else if event is TIDS timer then
For each neighbour CH
if selected as a voter then
execute voting based intrusion detection
else / / event is data packet arrival
Follow multipath routing protocol design to route the data packet.
```

Ch Execution for Dynamic Redundancy Management

```
SN Execution
Get next event
If event is TD timer then
determine radio range to maintain SN
connectivity within a cluster
```

```
else if event is control packet arrival from CH
then
change the optimal settings of TIDS, and m
else if event is T clustering timer then
perform clustering
else if event is TIDS timer then
For each neighbour SN
if selected as a voter then
execute voting based intrusion detection
else / / event is data packet arrival
Follow multipath routing protocol design to route the data packet.
Sn Execution for Dynamic Redundancy Management
```

VI. CONCLUSION

The research that we are formulating focuses on redundancy controlling to exploit the tradeoff between energy consumption vs the gain in reliability, timeliness by dynamic multipath routing to maximize the system useful lifetime. For these reasons, we formulate the acknowledgement system in between nodes, cluster heads, processing center and sink. When cluster heads sends data to the processing center and then to sink at that time sink will keep that path as reliable path in its logs and again sends acknowledgement to the senders end and considers this path as reliable for further transmission. So acknowledgement avoids this repeated transmission which results in conservation of energy by detecting and evicting malicious node in HWSN. Dynamic redundancy controlling algorithm to formulate and implement the best design parameters settings at runtime in response to environmental changes to maximize HWSN lifetime using logs created at sink. Lastly, we plan to investigate the use of trust/reputation management to strengthen intrusion detection through “weighted voting” leveraging knowledge of trust/reputation of neighbor nodes, as well as to tackle the “what paths to use” problem in multipath routing decision making for intrusion tolerance in WSNs. In situations where concurrent query traffic is heavy, we plan to explore trust-based admission control to optimize application performance.

REFERENCES

1. Improving the Fault Tolerance in Multipath Routing of Heterogeneous Wireless Sensor Networks.Sona Nelson1, N.Inzohan21.M.E, Computer Science and Engineering, Vel Tech Multi Tech Engineering College, Avadi, Chennai2.Assistant Professor, Department of Computer Science and Engineering, Vel Tech Multi Tech Engineering College,Avadi, Chennai.
2. Mohamed Mubarak T, Syed Abdul Sattar, G.AppaRao, Sajitha M,” Intrusion detection: An Energy efficient approach in Heterogeneous WSN,” in proc.2011 IEEE International Conference on Emerging Trends in Electrical and Computer Technology.
3. X. Du and F. Lin, “Improving routing in sensor networks with heterogeneous sensor nodes,” in Proc. 2005 IEEE Veh. Technol. Conf., pp 2528-2532.
4. Intrusion Dectection and Fault Tolerance in heterogeneous Wireless Sensor Network: A Survey, SnehaDhage, Purnima Soni Computer Science & Engineering, G.H. Raisoni Institute of Engineering and Technology for Women, Nagpur. International Journal of Scientific and Research Publications, Volume 4, Issue 2, February 2014 1 ISSN 2250-3153.
5. Ing-Ray Chen, Member, IEEE, AnhPhan Speer, and Mohamed Eltoweissy, Senior Member, IEEE Adaptive Fault-Tolerant QoS Control Algorithms for Maximizing System Lifetime of Query-Based Wireless Sensor Networks.
6. O. Younis and S. Fahmy, "HEED: a hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks," IEEE Trans. Mobile Comput., vol. 3, no. 4, pp. 366-379, 2004.
7. E. Felemban, L. Chang-Gun, and E. Ekici, "MMSPEED: multipath Multi-SPEED protocol for QoS guarantee of reliability and. Timeliness in wireless sensor networks," IEEE Trans. Mobile Comput., vol. 5, no. 6, pp.738-754, 2006.

8. I. R. Chen, A. P. Speer, and M. Eltoweissy, "Adaptive Fault-Tolerant QoS Control Algorithms for Maximizing System Lifetime of Query-Based Wireless Sensor Networks," IEEE Trans. on Dependable and Secure Computing, vol. 8, no. 2, pp. 161-176, 2011.
9. M. Yarvis, N. Kushalnagar, H. Singh, A. Rangarajan, Y. Liu, and S.Singh, "Exploiting heterogeneity in sensor networks," 24th Annu. Joint Conf. of the IEEE Computer and Communications Societies (INFOCOM), 2005, pp. 878-890 vol. 2.
10. H. M. Ammari and S. K. Das, "Promoting Heterogeneity, Mobility, and Energy Aware Voronoi Diagram in Wireless Sensor Networks," IEEE Trans. Parallel Distrib. Syst., vol. 19, no. 7, pp. 995-1008, 2008.
11. X. Du and F. Lin, "Improving routing in sensor networks with heterogeneous sensor nodes," IEEE 61st Vehicular Technology Conference, 2005, pp. 2528-2532.
12. S. Bo, L. Osborne, X. Yang, and S. Guizani, "Intrusion detection techniques in mobile ad hoc and wireless sensor networks," IEEE Wireless Commun., vol. 14, no. 5, pp. 56-63, 2007.