International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

Intrusion Detection System to Enhance the Performance in Multipath Routing for Heterogeneous Wireless Sensor Network

Tripti Manoj Shukla[1], Pankaj Salunkhe[2]

[1]M.E.EXTC, SES-Group of Institutions Faculty of Engineering, Bhivpuri Road, Karjat, Mumbai University (India)

[2]Professor, H.O.D(EXTC), SES-Yadavrao Tasgaonkar Institute of Engineering & Technology, Bhivpuri Road, Karjat, Mumbai University (India)

Abstract: ***In this paper we propose security of nodes by using Intrusion Detection System in heterogeneous wireless sensor networks (HWSNs) where we are utilizing multipath routing to answer user queries in the presence of unreliable and malicious nodes which causes packet loss in the network. The research problem we are addressing in this paper is to tolerate intrusions which are responsible for packet loss and jamming attack and security of each node . The main goal and objective of the paper is to enhance the performance in multipath routing to tolerate and detect intrusions & provide security to each node during transmission of data in the presence of intruders. The key concept of our redundancy management is to achieve the balance between energy consumption and gain in reliability, timeliness along with the security to maximize the system useful lifetime. In our work we have considered redundancy management of multipath routes which are based on trust and energy values and it is used for intrusion detection as well as to maximize the system lifetime of a HWSN in the presence of unreliable and malicious nodes. In this paper we are providing security at each node during the routing of data from source to sink, which is done by using RSA Algorithm which introduces cipher text as an encryption (AES) at each node. If intruder attacks any of the nodes, its code cannot be decrypted at the destination thus producing secured transmission of data.***

Keywords: Intrusion Detection System, Heterogeneous Wireless Sensor Networks, Multipath Routing, AES, Security, Encryption, Intrusion Tolerance

1. Introduction

Many wireless sensor networks (WSNs) are deployed in an unattended environment in which energy replenishment is difficult if not impossible. Due to limited resources, a WSN must not only satisfy the application specific QoS requirements such as reliability, timeliness and security, but also minimize energy consumption to prolong the system useful lifetime. The tradeoff between *energy* consumption vs. *reliability* gain with the goal to maximize the WSN system lifetime has been well explored in the literature. However, no prior work exists to consider the tradeoff in the presence of malicious attackers. It is commonly believed in the research community that clustering is an effective solution for achieving scalability, energy conservation, and reliability. Using homogeneous nodes in the roles of cluster heads (CHs) and sensor nodes (SNs) leveraging CH election protocols such as HEED **(**Hybrid Energy Efficient Distributed Clustering**)** for lifetime maximization and reducing the loss in data transfer has been considered.

Recent studies demonstrated that using heterogeneous nodes can further enhance performance and prolong the system lifetime. 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. The tradeoff issue between energy consumption vs. QoS gain becomes much more complicated when inside attackers are present as a path may be broken when a malicious node is on the path. This is especially the case in heterogeneous WSN (HWSN) environments in which CH nodes may take a more critical role in gathering and routing sensing data. Thus, very likely the system would employ an intrusion detection system (IDS) with the goal to detect malicious nodes. While the literature is abundant in intrusion detection techniques for WSNs, 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 (say to prevent a Byzantine failure) is largely unexplored. The issue is especially critical for energy constrained WSNs designed to stay alive for a long mission time. Multipath routing is considered an effective mechanism for fault and intrusion tolerance to improve data delivery 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. While most prior research focused on using multipath routing to improve reliability, some attention has been paid to using multipath routing to tolerate insider attacks. These studies, however, largely ignored the tradeoff between QoS gain vs. energy consumption which can adversely shorten the system lifetime. The research problem we are addressing here is effective redundancy management of a clustered HWSN to prolong its lifetime 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 the lifetime of a clustered HWSN while satisfying application QoS requirements in the context of multipath routing. More specifically, we analyze the optimal amount of redundancy through which data are routed to a remote sink in the presence of unreliable and malicious nodes, so that the query success probability is maximized while maximizing the HWSN lifetime. We consider this

optimization problem for the case in which a voting-based distributed intrusion detection algorithm is applied to remove malicious nodes from the 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.

Our major contribution is to provide security at each node during the routing of data from source to sink, which is done by using RSA Algorithm which introduces cipher text as an encryption (AES) at each node. If intruder attacks any of the nodes, its code cannot be decrypted at the destination thus producing secured transmission of data.

2. Analysis of Existing System

Many wireless sensor networks (WSNs) are deployed in an unattended environment in which energy replenishment is difficult if not impossible. Due to limited resources, a WSN must not only satisfy the application specific QoS requirements such as reliability, timeliness and security, but also minimize energy consumption to prolong the system useful lifetime. The trade-off between energy consumption vs. reliability gain with the goal to maximize the WSN system lifetime has been well explored in the literature. However, no prior work exists to consider the trade-off in the presence of malicious node.

In Existing systems:-

- In existing works no consideration was given to the existence of malicious node.
- In existing works no consideration was given to Energy Consumption & detection of Compromised node for Intrusion Detection.
- Very importantly no consideration was given to the security of each node during transmission of data in the presence of intruders.

A. Comparison of existing systems with proposed system

In Existing System, effective redundancy management of a clustered HWSN is used to prolong its lifetime 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 the lifetime of a clustered HWSN while satisfying application QoS requirements in the context of multipath routing. We are also using Advance Encryption Standards (AES) of 128 Bit Encryption to Encrypt data at each and every node of our HWSN which makes data more secure before transferring from each node. More specifically, we analyze the optimal amount of redundancy through which data are routed to a remote sink in the presence of unreliable and malicious nodes, so that the query success probability is maximized while maximizing the HWSN lifetime.

B. Detail Problem Definition

Many wireless sensor networks (WSNs) are deployed the environment where the energy replenishment is very difficult but it is not impossible. In WSN there are limited resources which are not only used to satisfy QoS requirement but also they must be useful to increase system lifetime with minimum energy consumption. So our aim is to solve the problem of balance between energy consumption, secure data transmission andQoS to provide reliability gain to maximize the WSN system lifetime. This is well explored in literature. However, inliterature no work exists to consider the tradeoff in the presence of malicious node which are responsible for packet loss also which are harmful to the network. It is considered that clustering is one of the best solutions to achieve the scalability, reliability and energy conservation in wireless sensor network. If the homogeneous network is consider then the cluster head (CH) is selected among all nodes which rotate in the network. Some of the protocol like HEED is used to elect cluster head among all available nodes in thenetwork, which are useful for lifetime maximization. Modern studies as given in suggest that use of heterogeneous nodes can also enhance performance in better way and prolong the system lifetime in. The nodes where highest resources such as highest residual energy is available will perform the role of CH and they are useful to perform computationally intensive task while inexpensive less capable SNs are utilized mainly for sensing the environment.

C. Justification of Problem

The steadiness between energy consumption with QoS requirement for reliability gain becomes much more difficult to manage when there is an inside attacker available in the network. This inside attacker will attack the sensor node and act as a malicious node and will be responsible to break the path in the network and will disturb the working of the network. This is the case which generally happens in heterogeneous WSN (HWSN) environments where CH nodes takes more critical role in routing as well as data gathering from the sensor nodes(SN) which are available in the network. Thus, it is essential to employ effective intrusion detection system (IDS) to detect as well as to remove such malicious nodes from the system. Also such IDS system must provide good performance with minimum energy consumption so that it is helpful to improve system lifetime. While in the literature there are number of intrusion detection techniques for WSN like, but the issue is how often the intrusion detection should be invoked to detect and remove malicious node from the system so that we can improve system useful lifetime. The issue is exclusively precarious for energy- constrained WSNs designed to stay alive for a long mission time. Another solution to increase system lifetime is to use multipath routing which is also for fault and intrusion tolerance to improve data delivery in WSNs. The basic idea is to increase the number of path toward the sink from every node available in the WSN. That is we need to enlarge the count of number of path reaching the sink node or base station. While most prior research focused on using multipath routing to improve reliability, some attention has been paid to using multipath routing to tolerate insider attacks. All the current studies, however, largely ignored the steadiness between QoS gain and energy consumption which can adversely shorten the system lifetime.

D. Need of Proposed System

The problem we are addressing in this report is effective redundancy management of a clustered HWSN to maximize system lifetime operation in the presence of unreliable and malicious nodes which are responsible for packet loss. We are addressing the trade-off issue between energy consumption with QoS requirement to gain in reliability and timeliness as well as to increase security so that we can maximize the lifetime of a clustered heterogeneous WSN, it will also be a satisfying application for QoS requirements in case of multipath routing. More specifically, we are analyzing the optimal amount of redundancy in WSN through which data are routed to a remote sink in the presence of unreliable and malicious nodes, so that the probability to answer users query must be maximized while maximizing the system lifetime. For the issue of intrusion tolerance through multipath routing, there are two major problems to solve first is how many paths to use and second is what paths to use. We are focusing on to address the how many paths to use to reach to the sink problem. Our approach is different from existing for the, what paths to use problem, in that we do not consider specific routing protocols (e.g., MDMP for WSNS or AODV for MANETs), nor the use of feedback information to solve the problem. Rather, we are employing a IDS by which intrusion detection is performed only locally so that there must be less energy conservation by the nodes in the network. The compromised nodes are detected and the path through that node is ignored from the heterogeneous WSN. In this paper we decide how many paths to use in order to tolerate residual compromised nodes that survive our IDS, so as to increase system useful lifetime of the HWSN. The contribution of our paper is that we explore more extensive malicious attacks in addition to packet loss attack and jamming attacks which occur because of packet dropping by malicious nodes, each with different implications to energy, security and reliability, and investigate intrusion detection and
multipath routing based tolerance protocols to react to these attacks.

3. Methodology

3.1 Concept

In the Proposed System we are addressing efficient redundancy management of a clustered HWSN to maximize system lifetime operation in the presence of unreliable and malicious nodes which are responsible for packet loss. We are addressing the balance between energy consumption with the QoS requirement to gain in reliability and timeliness as well as to increase security so that we can maximize the lifetime of a clustered heterogeneous WSN, it will also be a satisfying application for QoS requirements in case of multipath routing. In our work we have considered redundancy management of multipath routes which are based on trust and energy values and it is used for intrusion detection, and to maximize the system lifetime of a HWSN in the presence of unreliable and malicious nodes. Today's research challenge in WSNs is coping with low power communication. Routing protocols in this regard plays a key role in efficient energy utilization. In sending data from sensor nodes to BS there is need to select a specific route and must be a shortest route, which mange to minimize the energy consumption is necessary. Hence we are using clustering approach to minimize the energy consumption. In this paper we are using symmetric encryption technique to protect confidentiality. To increase security we have revealed more extensive attacks by the malicious nodes such as packet loss attack and jamming attack each assault is having altered energy requirement as well as security and reliability.

More specifically, we are analyzing the optimal amount of redundancy in WSN through which data are routed to a remote sink in the presence of unreliable and malicious nodes, so that the possibility to answer users query must be maximized while maximizing the system lifetime To tolerate intrusion through multipath routing, there are two major problems to solve first is how many paths to use and second is what paths to use. We are concentrating on to report the how many paths to use to reach to the sink problem. Our approach is different from existing for the, what paths to use problem, in that we do not consider specific routing protocols and we are not using any feedback information to solve the problem. Rather, we are employing IDS by which intrusion detection is performed only locally so that there must be less energy conservation by the nodes in the network. The compromised nodes are detected and the path through that node is ignored from the heterogeneous WSN. In this paper we decide which paths to use in order to tolerate residual compromised nodes that survive our IDS, so as to increase system useful lifetime of the HWSN. In this paper we also discover more extensive malicious attacks in addition to packet loss and jamming attacks which occur because of malicious nodes, each with different implications to energy, security and reliability, and investigate intrusion detection and multipath routing based tolerance protocols to react to these attacks.

4. System Model

A heterogeneous WSN consists of different types of sensors having different sensing capabilities. We have considered two types of sensor nodes, one is cluster head (CHs) and another is sensor node SNs. Cluster heads (CHs) are more superior than sensor nodes(SNs) in consideration of energy as well as computational resources. We are using heterogeneous network in which each node is having more amount of resources.

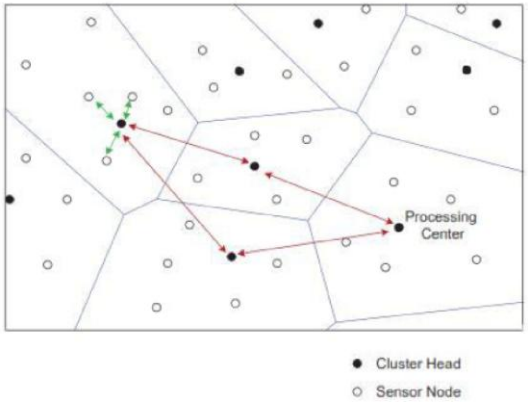

Figure 1

Redundancy management of multipath routing for intrusion tolerance in presence of malicious nodes is achieved through two forms of redundancy: (a) source redundancy by which ms SNs sensing a physical phenomenon in the same feature zone are used to forward sensing data to their CH (referred to as the source CH); (b) path redundancy by which mp paths are used to relay packets from the source CH to the base station through the use of neighboring CHs. Fig.1 shows a scenario with a source redundancy of 3 (m=3)

and a path redundancy of 2 (m=2). It has been reported that the number of edge-disjoint paths between nodes is equal to the average node degree with a very high probability. Therefore, when the density is adequately high such that the average number of one-hop neighbors is sufficiently larger than mp and ms, we can effectively result in m redundant paths for path redundancy and mp distinct paths from m sensors for source redundancy. We are assuming that geographic routing which is a well-known routing protocol for WSNs, is used to route the data from CH to the base station or sink along with multipath routing; thus, in this case there is no need to conserve path information of the network. We must know the location of the destination node so that we can correctly send the packet towards it. So the CH are responsible to get the location of all SN and vice versa in its cluster and it is the part of clustering. A CH is also aware with the location of neighbor CHs along with the direction towards the base station or sink. In this paper we are using clustering to reduce the energy consumption by the nodes to send data to the base station. Cluster is the group of Nodes and in the paper, we are grouping the nodes to form cluster. Here cluster formation is based on the specific region and the nodes located in the specified region. We are selecting the region with specific distance from the base station and then the area is selected and the nodes inside region are located and grouped. In this approach clusters are formed statically at the time of network deployment so all the sensor nodes and their CH nodes are selected. The Cluster Head is selected on the Highest Energy basis, the node which has maximum energy is selected as Cluster Head. We also assume that all the sensor nodes and cluster heads should operate in power saving mode so that less energy is utilized. Hence, a sensor is either active i.e. transmitting or receiving or it is in sleep mode. For the energy consumption while sending & receiving information we are using the energy model in for both CHs and SNs. To preserve confidentiality we are using AES symmetric key encryption algorithm. AES is Symmetric key Cryptographic algorithm. It is used to provide security in our paper. While sending data, a sensor node can encrypt data by using key encryption technique and then send that encrypted data to the CH so that it is helpful to achieve confidentiality and authentication. Then the data is transmitted and it will help to secure data from the attacker and packets are formed from the file and actually packets are transmitted. At the destination the data is decrypted by the destination node.

To detect compromised nodes from HWSN, we are using acknowledgement based IDS. When the forwarded data is received at the receiver side, then it sends acknowledgement to the sender node. The acknowledge ACK which is received is compared with the size of received data; if it is equal then data is forwarded successfully with no loss in packets; otherwise it will detect loss in the packet. Hence, it detects such a node as a malicious node due to which packet loss happens. This is applied to every node in the network and each node will assess its acknowledgement with the size of data received to detect the attack and compromised node in the WSN.

To detect jamming attack in network we are using a counter based approach if the counter goes beyond the threshold then it will detect that network is jammed. Here we have noted that increasing source redundancy as well as path redundancy will enhances the reliability and security. However, it also decreases the energy consumption and thus it contributing to the increase of the system lifetime. Thus, there is balance between gain in reliability and security with the less energy consumption. The dispersed IDS design attempts to detect and evict compromised nodes from the network without unnecessarily wasting energy so as to maximize the query success probability and the system lifetime.

A. What is Advanced Encryption Standard (AES)?

The Advanced Encryption Standard or AES is a symmetric block cipher used by the U.S. government to protect classified information and is implemented in software and hardware throughout the world to encrypt sensitive data.The origins of AES date back to 1997 when the National Institute of Standards and Technology (NIST)announced that it needed a successor to the aging Data Encryption Standard (DES) which was becoming vulnerable to brute-force attacks. This new encryption algorithm would be unclassified and had to be "capable of protecting sensitive government information well into the next century." It was to be easy to implement in hardware and software, as well as in restricted environments (for example, in asmart card) and offer good defences against various attack techniques.

B. Choosing AES

The selection process to find this new encryption algorithm was fully open to public scrutiny and comment; this ensured a thorough, transparent analysis of the designs. Fifteen competing designs were subject to preliminary analysis by the world cryptographic community, including the National Security Agency (NSA). In August 1999, NIST selected five algorithms for more extensive analysis. These were:

- MARS, submitted by a large team from IBM Research
- RC6, submitted by RSA Security
- Rijndael, submitted by two Belgian cryptographers, Joan Daemen and Vincent Rijmen
- Serpent, submitted by Ross Andersen, Eli Biham and Lars Knudsen
- Two fish, submitted by a large team of researchers including Counterpane's respected cryptographer, Bruce Schneier

Implementations of all of the above were tested extensively in ANSI, C andJava languages for speed and reliability in encryption and decryption, keyand algorithm setup time, and resistance to various attacks, both in hardware- and software-centric systems. Members of the global cryptographic community conducted detailed analyses

(including some teams that tried to break their own submissions). After much enthusiastic feedback, debate and analysis, the Rijndael cipher -- a mash of the Belgian creators' last names Daemen and Rijmen -- was selected as the proposed algorithm for AES in October 2000 and was published by NIST as U.S. FIPS PUB 197. The Advanced Encryption Standard became effective as a federal government standard in 2002. It is also included in the ISO/IEC 18033-3 standard which specifies block ciphers for the purpose of data confidentiality. In June 2003, the U.S. government announced that AES could be used to protect classified information, and it soon became the default encryption algorithm for protecting classified information as well as the first publicly accessible and open cipher approved by the NSA for top-secret information. AES is one of the Suite B cryptographic algorithms used by NSA's Information Assurance Directorate in technology approved for protecting national security systems. Its successful use by the U.S. government led to widespread use in the private sector, leading AES to become the most popular algorithm used in symmetric key cryptography. The transparent selection process helped create a high level of confidence in AES among security and cryptography experts. AES is more secure than its predecessors -- DES and 3DES -- as the algorithm is stronger and uses longer key lengths. It also enables faster encryption than DES and 3DES, making it ideal for software applications, firmware and hardware that require either low-latency or high throughput, such as firewalls and routers. It is used in many protocols such as SSL/TLS and can be found in most modern applications and devices that need encryption functionality.

C. How AES encryption works?

AES comprises three block ciphers, AES-128, AES-192 and AES-256. Each cipher encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128-, 192- and 256-bits, respectively. (Rijndael was designed to handle additional block sizes and key lengths, but the functionality was not adopted in AES.) Symmetric or secret-key ciphers use the same key for encrypting and decrypting, so both the sender and the receiver must know and use the same secret key. All key lengths are deemed sufficient to protect classified information up to the "Secret" level with "Top Secret" information requiring either 192- or 256-bit key lengths. There are 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys -- a round consists of several processing steps that include substitution, transposition and mixing of the input plaintext and transform it into the final output of ciphertext. We are using AES-128 in this project.

D. Algorithm for Intrusion Tolerance & attack detection

1: if(network created)
2: if(SourceNode != DestNode)
3: int Size = datasize;
4: Send(data)
5: ACK = data received size;
6: if(ACK == datasize)
7: Data received successfully;
8: Flag = true;
9: else
10: Data is lost in path;
11: Flag = false;
12: if(Flag == false)
13: For all paths;
14: Calculate average of energy and trust value.
15: if(average==maximum value)
16: shortest path = current path;
17: Send(data);

In proposed work, we are using multipath routing and encryption/Decryption technique. The fundamental obligation of the sensor nodes in each system is to sense the range and transmit their gathered data to the sink node for further operations. Multipath Routing is a routing procedure, which chooses various ways to convey information in the middle of source and destination nodes. As the essential significance of routing means, selecting best way in the system, multipath routing strategies are utilized to choose the best path in the network.

From the above algorithm, Firstly a network is created which consist of different clusters and based on energy levels of each node the cluster heads are elected. To forward a data within a HWSN distinct source node and destination nodes are selected. To increase system lifetime we have to detect malicious nodes which are responsible for different attacks such as packet loss and jamming attack. To detect compromised nodes from HWSN, we are using acknowledgement based IDS. When the forwarded data is received at the receiver side, then it sends acknowledgement to the sender node. The ACK is compared with the size of received data; if it is equal then data forwarded successfully with no loss in packets; otherwise it will detect loss in the packet. Hence, it detects such a node as a malicious node due to which packet loss happens. This is applied to every node in the network and each node will assess its acknowledgement with the size of data received to detect the attack and compromised node in the WSN.

5. System Specifications

Hardware Requirements:

- System : Pentium IV 2.4 GHz.
- Hard Disk : 40 GB.
- Floppy Drive: 1.44 Mb.
- Monitor : 15 VGA Color.
- Mouse : Logitech.
- Ram : 512 Mb.

Software Requirements:

- Operating system :-Windows 7 Ultimate (32-bit) / Windows XP
- Coding Language : C#.Net
- Front End: Visual Studio 2010

6. Implementation

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective. The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

A. Modules

1. Multi – Path Routing
2. Intrusion Tolerance
3. Energy Efficient
4. Simulation Process

Modules Description:

1) **Multi – Path Routing:** In this module, Multipath routing is considered an effective mechanism for fault and intrusion tolerance to improve data delivery in WSNs. The basic idea is that the probability of atleast one path reaching the sink node or base station increases as we have more paths doing data delivery. While most prior research focused on using multipath routing to improve reliability, some attention has been paid to using multipath routing to tolerate insider attacks. These studies, however, largely ignored the tradeoff between QoS gain vs. energy consumption which can adversely shorten the system lifetime.
2) **Intrusion Tolerance:** In this Modules, intrusion tolerance through multipath routing, there are two major problems to solve:
   a) How many paths to use and
   b) What paths to use.

   To the best of our knowledge, we are the first to address the "how many paths 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 Efficient:** In this module, there are two approaches by which energy efficient IDS can be implemented in WSNs. One approach especially applicable to flat WSNs is for an intermediate node to feedback maliciousness and energy status of its neighbor nodes to the sender node (e.g., the source or sink node) who can then utilize the knowledge to route packets to avoid nodes with unacceptable maliciousness or energy status. Another approach which we adopt in this paper is to use local host-based IDS for energy conservation.
4) **Simulation Process:** In this module, the cost of executing the dynamic redundancy management algorithm described above, including periodic clustering, periodic intrusion detection, and query processing through multipath routing, in terms of energy consumption.

7. Results and Discussion

The aim of our system is to increase lifetime and security in the network. To evaluate the performance we need to use different metrics. In our work we are using following metrics:

(i) Data Transfer Time
(ii) Data Delivery Ratio

The following graph of data transfer time required for communication, in this graph we shows three types of communication with Jamming, with MIM attack and with Normal communication and the time required for the communication. Lifetime is depending on the Energy of the network and as the energy consumption depends on the node processing time. The jamming attack and MIM attack requires more time for processing and it consumes more energy and If we are using the same path for communication then we are wasting unnecessary energy and hence node may cause dead hence to avoid this we are changing the path and after the path change the data transfer time is less as compared to attack. Hence the minimum time requires minimum energy and indirectly the network lifetime is increased by path changed for communication.

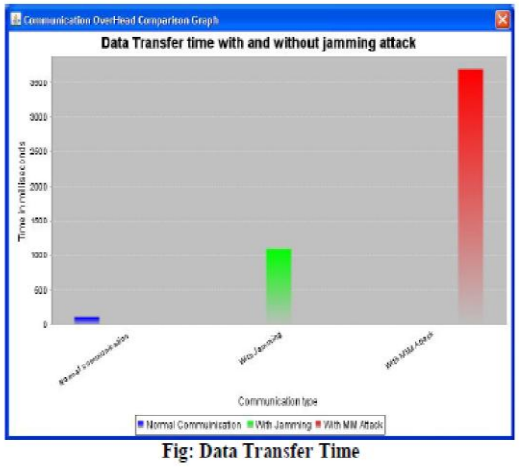

Fig: Data Transfer Time

Algorithms	Data Transmission Time
MIM attack	3703
Jamming Attack	1343
Proposed System	100

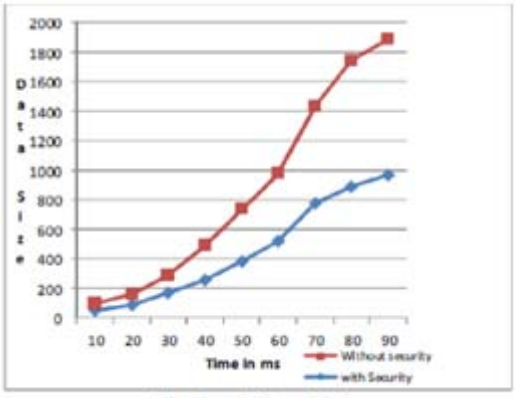

Fig: Data Delivery Ratio

Time in ms	Data size With security	Data size Without security
10	53	42
20	88	73
30	168	125
40	258	230
50	386	350
60	522	456
70	780	658

The aim of our system is to increase lifetime and security in the network, in the first graph we shows that how we increased lifetime and this graph shows the time required for sending the specific size of data with and without security, as we are providing the security the time should be more as compared to normal sending for security we are using the encryption algorithm (AES) for security.

8. Conclusion

In this report we have performed a trade-off analysis of energy consumption and QoS requirement to reliability gain and timeliness as well as to provide security for redundancy management of clustered heterogeneous wireless sensor networks by utilizing multipath routing to answer user queries. In our work, we consider redundancy management of multipath routes, based on trust and energy values, for intrusion detection, and to maximize the system lifetime of a HWSN in the presence of unreliable and malicious nodes. we have noted that increasing source redundancy as well as path redundancy will enhances the reliability and security. However, it also decreases the energy consumption and thus it contributing to the increase of the system lifetime. The proposed hierarchical dynamic trust management protocol for cluster-based wireless sensor networks, considering two aspects of trustworthiness, namely, social trust and QoS trust. The research work will include the development of a probability model utilizing various techniques to analyze the protocol performance, and validated subjective trust against objective trust obtained based on ground truth node status. Based on the protocol the algorithm for trust-based intrusion detection will be developing using weighted voting. The algorithm will identify the best way to form trust out of social and QoS trust properties (i.e., identifying weights to assign to individual trust properties) and to assign the minimum trust threshold, so that the performance of trust-based intrusion detection is maximized, i.e., both false positives and false negatives are minimized. We performed a tradeoff analysis of energy consumption vs. QoS gain in reliability, timeliness, and security for redundancy management of clustered heterogeneous wireless sensor networks utilizing multipath routing to answer user queries. We developed a novel probability model to analyze the best redundancy level in terms of path redundancy (mp) and source redundancy (m), as well asthe best intrusion detection settings in terms of the number of voters (m) and the intrusion invocation interval (s) under which the lifetime of a heterogeneous wireless sensor network is maximized while satisfying the reliability, timeliness and security requirements of query processing applications in the presence of unreliable wireless communication and malicious nodes. Finally, we applied our analysis results to the design of a dynamic redundancy management algorithm to identify and apply the best design parameter settings at runtime in response to environment changes to prolong the system lifetime.

9. Bibliography

Good Teachers are worth more than thousand books, we have them in Our Department

References

[1] Hamid Al-Hamadi and Ing-Ray Chen, "Redundancy Management of Multipath Routing for Intrusion Tolerance in Heterogeneous Wireless Sensor Networks," IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT, VOL. 10, NO. 2, JUNE 2013.
[2] 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.
[3] E. Felemban, L. et al, "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.
[4] I. R. Chen, et.al, "Adaptive fault-tolerant QoS control algorithms for maximizing system lifetime of query-based wireless sensor networks," IEEE Trans. Dependable Secure Computing, vol. 8, no. 2, pp. 161–176, 2011.
[5] M. Yarvis, N. Kushalnagar, H. Singh, A. Rangarajan, Y. Liu, and S.Singh, "Exploiting heterogeneity in sensor networks," in Proc. 2005 IEEE Conf. Computer Commun., vol. 2, pp. 878–890
[6] 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.
[7] X. Du and F. Lin, "Improving routing in sensor networks with heterogeneous sensor nodes," in Proc. 2005 IEEE Veh. Technol. Conf., pp. 2528–2532.
[8] S. Bo, L. Osborne, X. Yang, and S. Guizani, "Intrusion detection techniques in mobile ad hoc and wireless sensor networks," IEEE Wireless Commun. Mag., vol. 14, no. 5, pp. 560–563, 2007
[9] I. Krontiris, T. Dimitriou, and F. C. Freiling, "Towards intrusion detection in wireless sensor networks," in Proc. 2007 European Wireless Conf.
[10] J. H. Cho, I. R. Chen, and P. G. Feng, "Effect of intrusion detection on reliability of mission-oriented mobile group systems in mobile ad hoc networks," IEEE Trans. Reliab., vol. 59, no. 1, pp. 231–241, 2010.
[11] A. P. R. da Silva, M. H. T. Martins, B. P. S. Rocha, A. A. F. Loureiro, L.B. Ruiz, and H. C. Wong, "Decentralized intrusion detection in wireless sensor networks," in Proc. 2005 ACM Workshop Quality Service Security Wireless Mobile Net.
[12] Y. Zhou, Y. Fang, et.al., "Securing wireless sensor networks: a survey," IEEE Commun. Surveys & Tutorials, vol. 10, no. 3, pp. 6–28, 2008.

[13] L. Lamport, et. al, "The byzantine generals problem," ACM Trans. Programming Languages Syst., vol. 4, no. 3, pp.382–401, 1982
[14] Y. Yang, C. Zhong, Y. Sun, and J. Yang, "Network coding based reliable disjoint and braided multipath routing for sensor networks," J. Netw. Comput.Appl., vol. 33, no. 4, pp. 422–432, 2010.
[15] J. Deng, et. al, "INSENS: intrusion-tolerant routing for wireless sensor networks," Computer Commun., vol. 29, no. 2, pp. 216–230, 2006
[16] K. D. Kang, K. Liu, and N. Abu-Ghazaleh, "Securing geographic routing in wireless sensor networks," in Proc. 2006
[17] W. Lou and Y. Kwon, "H-SPREAD: a hybrid multipath scheme for secure and reliable data collection in wireless sensor networks," IEEE Trans. Veh. Technol., vol. 55, no. 4, pp. 1320–1330, 2006.