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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 5, May 2014

Secure Multipath Routing For Energy Efficiency and Intrusion Tolerance in WSN

Shruti.S.Kumar

Dept of Computer Science and Engineering, M.S Ramaiah Institute of Technology, Bangalore, India

Abstract: This Paper Aims to find an effective mechanism to transmit the data from Source to the destination in the presence of malicious node, without the data being compromised, minimizing the energy Consumed and maximizing the lifetime of the system. A Light Weight Voting Based IDS is performed to evict the malicious node. Authenticity of message is preserved using Pair wise Key Establishment Protocol and HOP-HOP Message Authentication**.** The Work aims at achieving a tolerance to both inside and outside attackers in WSN.

Keywords: Intrusion, VotingBased IDS, Clustering, Heterogeneous

I. INTRODUCTION

Wireless sensor networks (WSNs) are deployed in an unattended environment. These miniature nodes are extremely small, as tiny as a cubic centimetre. Compared with conventional computers, the low-cost, battery-powered, sensor nodes have a limited energy supply, stringent processing and communications capabilities, and memory is scarce. The design and implementation of relevant services for WSNs must keep these limitations in mind. Based on the collaborative efforts of a large number of sensor nodes, WSNs have become good candidates to provide economically viable solutions for a wide range of applications, such as environmental monitoring, scientific data collection, health monitoring, and military operations. As Specified, one of the major Drawback of WSN is Limited Resources. Meanwhile satisfying the QOS In order to Minimize the Energy Consumed, to maximize the Lifetime of the System is a Challenge. The issue is especially critical for energy constrained WSNs designed to stay alive for a long mission time. One of the effective solution for achieving scalability, energy conservation, and reliability is clustering.

Clustering provides an effective mechanism for extending the lifetime of a sensor network. Each cluster elects one node as the cluster head. Data collected from sensors are sent to the cluster head first, and then forwarded to the sink. Cluster heads can fuse data from sensors to minimize the amount of data to be sent to the sink. When network size increases, clusters can also be organized hierarchically.

Homogeneous nodes rotate among themselves in the roles of cluster heads (CHs) and sensor nodes (SNs) leveraging CH election protocols such as HEED to Maximize the Lifetime of the System. Recent studies demonstrated that using heterogeneous nodes can further enhance performance and prolong the system lifetime. Here, nodes with superior resources serve as CHs, performing computationally intensive tasks while inexpensive less capable SNs are utilized mainly for sensing the environment.

Energy consumption v/s QOS gain is considered as an Issue in the Presence of Malicious node. In Heterogeneous WSN, CH node is Responsible for gathering and Routing the Sensing data, where more computational work is involved. Therefore when there is a malicious node in the path, energy consumed by the network will be more than expected. Thus an Intrusion detection system (IDS) must be deployed, that can detect and evict the malicious node. Running IDS is again energy Consumption. Therefore we need to deploy a timer that will determine how periodically the IDS should run.

The rest of the paper is organized as follows. In Section II we discuss related work and contrast our approach with existing work and we discuss about Intrusion, Energy Efficient Multi path Routing, Message Authentication and PIKE. In Section III we discuss about the System Model we implement and Pseudocode. Finally in Section IV we conclude the paper.

II. RELATED WORK

An easy way to comply with the conference paper formatting requirements is to use this document as a template and simply type your text into it. In the context of secure multipath routing for intrusion tolerance, [6] provides an excellent survey in this topic. In [7] the authors considered a multipath routing protocol to tolerate black hole and selective forwarding attacks. The basic idea is to use overhearing to avoid sending packets to malicious nodes.

Over the past few years, numerous protocols have been proposed to detect intrusion in WSNs. In [8], a decentralized rule based intrusion detection system is proposed by which monitor nodes are responsible for monitoring neighbouring nodes.

The monitor nodes apply predefined rules to collect messages and raise alarms if the number of failures exceeds a threshold value. Our host IDS essentially follows this strategy, with the flaws of the host IDS characterized by a false positive probability (Hpfp) and a false negative probability (Hpfn). In [10], however, no consideration is given about bad-mouthing attacks by compromised monitor nodes themselves, so if a monitor node is malicious, it can quickly infect others.

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 5, May 2014

A. Intrusion

WSN are often deployed in potentially adverse or even hostile environments. Therefore, they cannot be readily deployed without first addressing security challenges. One of the most important purposes of deploying WSNs is to collect relevant data. In a data collection process, aggregation was required to save energy, thus prolonging the lifetime of a WSN. However, aggregation primitives are vulnerable to node compromise attacks. This leads to falsely aggregated results by a compromised aggregator. Hence, effective techniques are required to verify the integrity of aggregated results. Prevention-based approaches can significantly reduce potential attacks. However, they cannot totally eliminate intrusions. Once a node is compromised, all the secrets associated with the node are open to attacks. This renders prevention- based techniques less helpful for guarding against malicious insiders. In practice, insiders can cause much greater damage.

An intrusion is defined as a set of actions that compromises confidentiality, availability, and integrity of a system. There are basically two types of intrusion detection: misuse-based detection and anomaly based detection [3]. A misuse-based detection technique encodes known attack signatures and system vulnerabilities and stores them in a database. If deployed IDS find a match between current activities and signatures, an alarm is generated. Misuse detection techniques are not effective to detect novel attacks because of the lack of corresponding signatures.

An anomaly-based detection technique creates normal profiles of system states or user behaviours and compares them with current activities. If a significant deviation is observed, the IDS raise an alarm. Anomaly detection can detect unknown attacks. However, normal profiles are usually very difficult to build.

Specification based detection techniques combine the advantages of misuse detection and anomaly detection by using manually developed specifications to characterize legitimate system behaviours. Specification-based detection approaches are similar to anomaly detection techniques in that both of them detect attacks as deviations from a normal profile. However, specification-based detection approaches are based on manually developed specifications, thus avoiding the high rate of false alarms. However, the downside is that the development of detailed specifications can be time-consuming.

The unique characteristics of sensor nodes pose challenges to the construction of a WSN IDS. A WSN has a limited power supply, thus requiring energy-efficient protocols and applications to maximize the lifetime of sensor networks. Sensor nodes have stringent system resources in terms of memory and computational capabilities, making intensive calculations impractical. Sensor nodes are prone to failure. This results in frequent network topology changes. 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.

In general 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 neighbour 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, is to use local host-based IDS for energy conservation (with SNs monitoring neighbour SNs and CHs monitoring neighbour CHs only), coupled with voting to cope with node collusion for implementing IDS functions. Energy efficiency is achieved by applying the optimal detection interval to perform IDS functions. Our solution considers the optimal IDS detection interval that can best balance intrusion accuracy vs. energy consumption due to intrusion detection activities and message authentication, so as to maximize the system lifetime. Voting based IDS approach considers the tradeoffs between energy loss vs. security and reliability gain with the goal to prolong the system lifetime.

B. Energy Efficient Multipath Routing

In “An Energy Efficient Multipath Routing Algorithm for Wireless Sensor Networks” Paper introduce a new routing algorithm for wireless sensor networks. The aim of this algorithm is to provide on-demand multiple disjoint paths between a data source and a destination. Multipath On-Demand Routing (MDR) is an on demand algorithm, meaning that a new path from a source to a destination is created only when a data packet has to travel between them. It is well suited for wireless sensor networks because it requires small communication overhead and low processing power. As the network diameter grows, data generated by one or more sources usually has to be routed through several intermediate nodes to reach the destination due to the limited range of each node’s wireless transmission. Problems arise when intermediate nodes fail to forward the incoming messages. To prevent this, acknowledgements and retransmissions are implemented. However, this generates large amount of additional traffic and delays in the network. The reliability of the system can be increased by using multipath routing [1].

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 MDR was designed with the goal of providing several disjoint paths between the source and the destination. It proved that it is tolerant to failures and more than that, it is almost immune to topology changes due to mobility. High average speeds of the nodes produce negligible negative effects. It is based on an initial flooding of the network with the route request and then generates route replies from the destination back to the source.

There are two phases:

- *Route Request* - when the source wants to find a destination it floods the network with a short message

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 5, May 2014

announcing this. The message contains the source ID, the destination ID and the ID of the request. Thus, the length of the message remains constant during the route request.

- *Route Reply* - the destination will eventually receive one of the route request messages. It only knows that there exists a path and it is not interested in what the path is. The destination just returns a route reply to the neighbour from which it received the route request message. The message contains a supplementary field that indicates the number of hops it travelled so far. Each node that receives a route reply, increments the hop count of the message and then forwards the message to the neighbour from which it got the original route request.

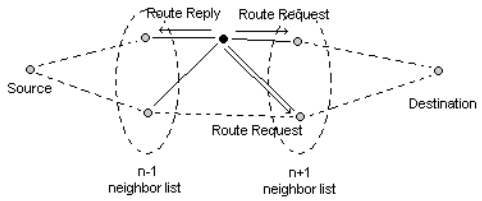

Fig 1 Request-Reply in multipath Routing

C. Message Authentication

Message authentication is one of the most effective ways to thwart unauthorized and corrupted messages from being forwarded in wireless sensor networks (WSNs). For this reason, many message authentication schemes have been developed, based on either symmetric-key cryptosystems or public-key cryptosystems. Most of them, however, have the limitations of high computational and communication overhead in addition to lack of scalability and resilience to node compromise attacks. Message authentication plays a key role in thwarting unauthorized and corrupted messages from being forwarded in networks to save the precious sensor energy. For this reason, many authentication schemes have been proposed to provide message authenticity and integrity verification for wireless sensor networks (WSNs).

These schemes can largely be divided into two categories: public-key based approaches and symmetric-key based approaches. The symmetric-key based approach requires complex key management, lacks of scalability, and is not resilient to large numbers of node compromise attacks since the message sender and the receiver have to share a secret key. The shared key is used by the sender to generate a message authentication code (MAC) for each transmitted message. However, for this method, the authenticity and integrity of the message can only be verified by the node with the shared secret key, which is generally shared by a group of sensor nodes. An intruder can compromise the key by capturing a single sensor node. In addition, this method does not work in multicast networks. To solve the scalability problem, a secret polynomial based message authentication scheme was introduced. However, when the number of messages transmitted is larger than the threshold, the polynomial can be fully recovered and the system is completely broken.

For the public-key based approach, each message is transmitted along with the digital signature of the message generated using the sender's private key. Every intermediate forwarder and the final receiver can authenticate the message using the sender's public key. One of the limitations of the public key based scheme is the high computational overhead. The recent progress on elliptic curve cryptography (ECC) shows that the public-key schemes can be more advantageous in terms of computational complexity, memory usage, and security resilience, since public-key based approaches have a simple and clean key management.

We use an unconditionally secure and efficient source anonymous message authentication (SAMA) scheme based on the optimal modified ElGamal signature (MES) scheme on elliptic curves.

D. PIKE

Peer Intermediaries for Key Establishment (PIKE), [5] is a key-establishment protocol that involves using one or more sensor nodes as a trusted intermediary to facilitate key establishment. Communication is an important requirement in many sensor network applications, so shared secret keys are used between communicating nodes to encrypt data. Since predetermining the potential location or connectivity of sensor nodes in a large deployment can be impractical, simply preloading each sensor node with the relevant shared keys cannot be considered. Key establishment protocols are used to set up the shared secrets, but the problem is complicated by the sensor nodes' limited computational capabilities, battery energy, and available memory.

PIKE uses sensor nodes as trusted intermediaries to establish shared keys between nodes. Each node shares a different (unique) pair wise key with each of other nodes in the network. The keys are deployed such that for any two nodes X and Y, it is possible to find some node Z in the network that shares a unique pair wise key with both X and Y. X can then securely route the key establishment message through Z to Y. Since unique pair wise keys that are shared between two nodes are redistributed, the established key is secure if Z has not been compromised by the adversary. Each key is unique and shared only between two nodes; hence they are called pair wise keys. For example, (x; y) will share a key K(x;y);(1;y) with (1; y) and a different key K(x;y);(2;y) with (2; y) and so on.
The two sets of nodes that share keys with any given node are the nodes that lie on the same row as X, and the same column as X, respectively.

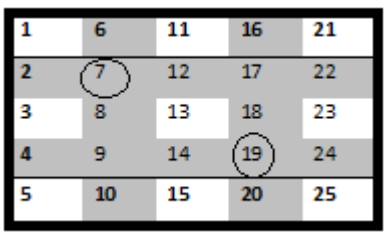

Fig 2 PIKE for n=25

Let number of nodes is 25.In this example, each number represents a node ID Shaded part indicate nodes which

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 5, May 2014

share unique keys with nodes 7 and 19 respectively. The keys are pair wise-shared and not common to a row; for example 15 and 01 share a key that is distinct from the key shared between 10 and 7 .Suppose node 17 wishes to perform key establishment with node 9. They both share unique pair wise keys with node 19 .Since node 19 lies on the same row as node 9 and the same column as node 17. Likewise, node7 is a valid intermediary since it lies on the same column as node 9 and the same row as node 17. If two neighboring nodes happen to have IDs that lie on the same row or same column then they already share a unique pair wise key and do not need to perform further key establishment. Once the IDs of the possible intermediaries have been found, the node initiating the key establishment chooses an intermediary through which to route the key-establishment message. It bases this choice on which of the two intermediaries has the smallest routing metric (or heuristic) for the path that the message will take.

III. SYSTEM MODEL

A HWSN comprises sensors of different capabilities. We consider two types of sensors: CHs and SNs. CHs are superior to SNs in energy and computational resources. Due to limited energy, a packet is sent hop by hop. All sensors are subject to capture attacks, i.e., they are vulnerable to physical capture by the adversary after which their code is compromised and they become inside attackers. Since all sensors are randomly located in the operational area, the same capture rate applies to both CHs and SNs, and, as a result, the compromised nodes are also randomly distributed in the operation area.

A CH which takes a query to process is called a query processing centre (PC).Many mission critical applications, e.g., emergency rescue and military battlefield, have a deadline requirement. We assume that each query has a strict timeliness requirement (Treq). The query must be delivered within Treq seconds; otherwise, the query fails.
As part of clustering, a CH knows the locations of SNs within its cluster, and vice versa. A CH also knows the location of neighbour CHs along the direction towards the processing centre. Multipath routing for intrusion tolerance 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 PC through intermediate CHs.

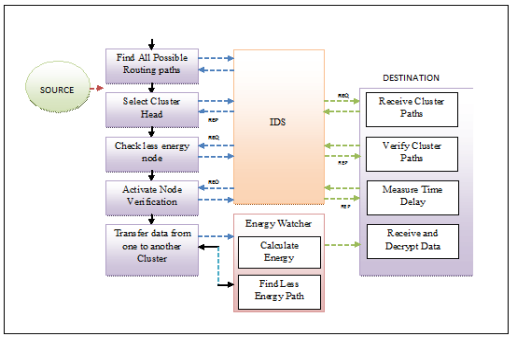

Fig 3 System Architecture

To preserve confidentiality, we need to perform Cryptography. Asymmetric cryptography such as RSA or Elliptic Curve cryptography (ECC) is unsuitable for most sensor architectures due to high energy consumption and increased code storage requirements. Overhead in communication and memory can be avoided using PIKE[5],where n nodes in the network shares a unique pair wise key with every other node in the network. We assume that the HWSN executes a pairwise key establishment protocol within each cluster after a Specific Interval of time from deployment.

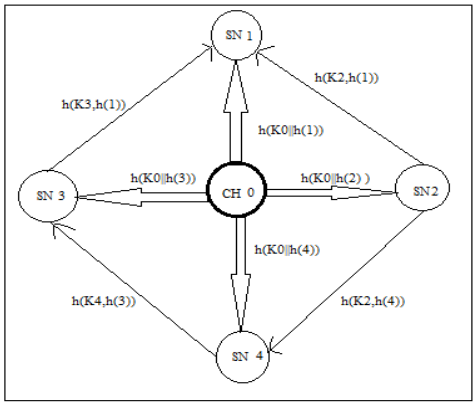

Fig 4 PIKE for each Cluster

In Each cluster, every SN node establishes pairwise keys with its k-hop SN neighbours, where k is large enough to cover a cluster area. Thus, when SNs join a new cluster, the CH node will have pairwise keys with the SNs joining its cluster. Since every SN shares a pairwise key with its CH, a SN can encrypt data sent to the CH for confidentiality and authentication purposes. This mechanism is useful to prevent outside attackers, not inside attackers.

In Order to prevent both inside and outside attackers, every CH node performs a Hop by Hop Message Authentication [3] protocol. It proposes an unconditionally secure and efficient source anonymous message authentication (SAMA) scheme based on the optimal modified ElGamal signature (MES) scheme on elliptic curves. This MES scheme is secure against adaptive chosen-message attacks in the random oracle model]. It enables the intermediate nodes to authenticate the message so that all corrupted message can be detected and dropped to conserve the sensor power.

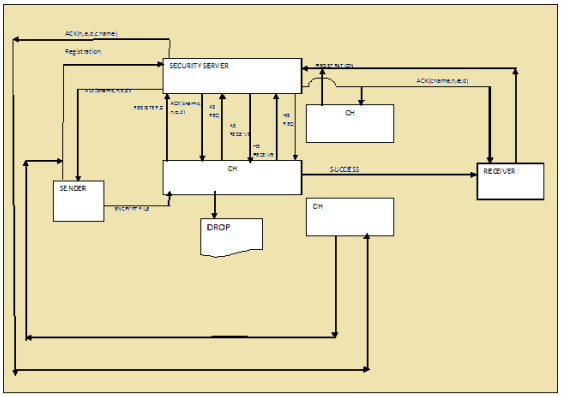

Fig 5 CH-CH Message Authentication

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 5, May 2014

Here they assume that, there exists a security server (SS) that is responsible for generation, storage and distribution of the security parameters among the network. This server will never be compromised. However, after deployment, the sensor nodes may be captured and compromised by attackers.

To detect compromised nodes, every node runs a simple host IDS to assess its neighbours. Host IDS is light-weight to conserve energy. It is also generic and does not rely on the feedback mechanism tied with any specific routing protocol .It is based on local monitoring. That is, each node monitors its neighbour nodes only. Each node uses a set of anomaly detection rules. If the count exceeds a system-defined threshold, a neighbour node that is being monitored is considered compromised. To remove malicious nodes from the system, a voting-based distributed IDS is applied periodically in every TIDS time interval. A CH is being assessed by its neighbour CHs, and a SN is being assessed by its neighbour SNs. In each interval, m neighbour nodes (at the CH or SN level) around a target node will be chosen randomly as voters and each cast their votes based on their host IDS results to collectively decide if the target node is still a good node. The m voters share their votes through secure transmission using their pairwise keys. When the majority of voters come to the conclusion that a target node is bad, then the target node is evicted.

For the issue of intrusion tolerance through multipath routing, there are two major problems to solve: (1) how many paths to use and (2) what paths to use. For the "what paths problem, we consider energy Efficient Multipath algorithm[1].Other than these for energy conservation, we have distributed light-weight IDS by which intrusion detection is performed only locally. Nodes that are identified compromised are removed from the HWSN. Only compromised nodes that survive detection have the chance to disturb routing.

A. Pseudocode:

Here, Treq is the lifetime of the Query. Tids is the regular interval at which IDS should Run. Let d be the data to transmit. $h(K_{s,}h(SN_{Neighbour,s}))$is the Pairwise key shared between Sender and Neighbour node. $h(K_{des)},h(SN_{Neighbour,des}))$ is the Pairwise key shared between Destination and its Neighbour node. Ms Source Redundancy and Mp Path Redundancy

1. $D=E(Data,h(K_{s,}h(SN_{Neighbour,s})))$
2. Send D
3. WhileT_{req} >0
4. While T_{ids} is ON
5. Execute Voting Based Algorithm
6. If Node Compromised
7. Eliminate Node
8. Reconstruct the path using Ms and Mp
9. End If
10. If d:SN->SN
11. Encrypt and Decrypt using Pair wise Key Distribution Protocol
12. End If
13. If d:CH->CH
14. Encrypt and Decrypt using Hop-Hop message Authentication
15. End if
16. Calculate System Energy
17. Do Loop
18. Do Loop
19. $Data=Decrypt(D,h(K_{des)},h(SN_{Neighbour,des})))$

IV. CONCLUSION

In this paper we propose to Achieve, Intrusion tolerance for Multipath Routing in the presence of Malicious Node by Conserving the Energy of the System and Maximizing its Liftetime. In addition we also focused on authenticating the Message transmitted by performing PIKE and HOP-HOP Message authentication.

REFERENCES

[1] Stefan Dulman, Jian Wu and Paul Havinga, "An Energy Efficient Multipath Routing Algorithm for Wireless Sensor Networks,"

[2] 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.

[3] Jian Li ,Yun Li ,Jian Ren and Jie Wu "Hop-by-Hop Message Authentication and Source Privacy in Wireless Sensor Networks" Ieee transac tions on mobile computing, vol. 12, no. 6, april 2013.

[4] Bo sun and lawrence osborne, lamar universityYang xiao, the university of alabamaSghaier guizani, university of quebec at trois-rivieres "intrusion detection techniques in mobile ad hoc and wireless sensor networks " scurity in wireless mobile adhoc and sensor networks

[5] C. Haowen and A. Perrig, "PIKE: peer intermediaries for key establishmentin sensor networks," in Proc. 2005 IEEE Conf. Computer Commun., pp. 524–535.

[6] E. Stavrou and A. Pitsillides, "A survey on secure multipath routingprotocols in WSNs," Comput. Netw., vol. 54, no. 13, pp. 2215–2238,2010.

[7] K. D. Kang, K. Liu, and N. Abu-Ghazaleh, "Securing geographic routingin wireless sensor networks," in Proc. 2006 Cyber Security Conf. Inf.Assurance.

[8] 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 SecurityWireless Mobile Netw.