ISSN: 2277-9655
Impact Factor: 1.852

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

Study on Secure Data Transmission through Dual-Path Rating Mechanism

Safia Fatima[*1], Dr. Abdul Waheed[2]

[*1]Research Scholar, JJT University Jhunjhunu Rajasthan, India

[2] Associate Professor, VTU Regional Office, Gulbarga, Karnataka, India

safiafatima95@yahoo.in

Abstract

In this paper, we propose a mechanism which would work on real time network environment and split the data before making transmission and merge the data before presenting to the user. The main objective of this paper is to study and analyse information security problem while the data is being transmitted over a network and propose a technique that will solve most of the hacking problem by attackers.

In this approach we divide the information packets flowing through a single path to flow through two different paths and reach destination. When information leaves the source machine it will be split into 2 parts and take 2 different routes to reach destination machine. After reaching destination again the packets will be combined and presented to the user. Thus providing a reliable way of data transmission while maintaining Data Integrity.

Keywords: CN, DoS, SMT, DWSN, DSR, MPTC, PRP, NRRP, DRP.

Introduction

Whenever the user is using a wireless sensor network, there will numerous security threats. In this paper we are mainly concentrating on combating two such threats [1][2]:

a) Compromised-node (CN) assault.

The Compromised-node assault is a condition where in an opponent has a separation of network machines for eavesdropping the data whenever it is transmitted.

b) Denial-of-service (DOS) assault.

In case of Denial-of-service attack, adversary mainly interferes with the normal operation by changing the functionality of subset of nodes, disrupting the functionality and so on [3].

These two types of attacks are almost similar since they both generate black holes. A black hole is an area within which the adversary can disrupt the nodes actively or block the information from transmitting. Since the wireless sensor networks are incapable from stopping generating the black holes, whenever there is severe CN attack or DOS attack, these black holes disrupts normal data delivery between the nodes [4].

The traditional cryptographic methodologies alone can't provide solutions to any of the problems like this. This is due to the fact that, one if at all if the nodes are compromised; the adversary can always capable of acquiring either the encryption/decryption keys of particular node. Along with that, the adversary can also perform some type of DOS attack even though if it doesn't have the knowledge of the cryptosystems which are used in the wireless sensor network.

For encountering this problem, one of the available solutions is exploiting the network's routing functionality.

In this paper, we mainly explore the potential for random dispersion of information in case of wireless sensor networks. Here, conditional on the information kind which is obtainable to sensor, 4 shared plans will be generated in favour of broadcasting information. The four different schemes are: [5]

1. purely random propagation
2. Non –recurring random broadcast
3. Multicast tree aided random broadcast.
4. Directed random propagation.

The PRP works by utilizing merely single hop area information as well as then furnishes the baseline information. The DRP methodology uses two-area data and provides the baseline performance. In case of MTRP it propagates shares or packets of information in the way of sink, thus creating the complete release procedure power competent.

ISSN: 2277-9655
Impact Factor: 1.852

Related Work

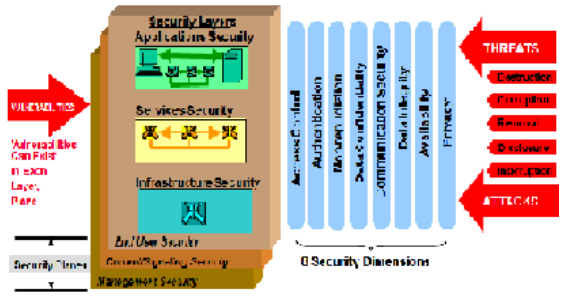

Figure 1: Security Architecture.

The concept of multi-path routing dates back to early 80s, when it was initially proposed to spread the traffic for the purpose of load balancing and throughput enhancement. Later on, one of its sub-classes, path-disjoint multi-path routing, has attracted a lot of attention in wireless networks due to its robustness in combating security issues.

a. Classification of Related Work

The related work can be classified into three categories. The first category studies the classical problem of finding node-disjoint or edge-disjoint paths. Some examples include the Split Multiple Routing protocol (SMR), multi-path DSR, and the AOMDV and AODMV algorithms that modify the AODV for multi-path functionality.

The second category includes recent work that explicitly takes security metrics into account in constructing routes. Specifically, the SPREAD algorithm in attempts to find multiple most-secure and node-disjoint paths. The security of a path is defined as the likelihood of node compromise along that path, and is labeled as the weight in path selection. A modified Dijkstra algorithm is used to iteratively find the top-K most secure node-disjoint paths. The H-SPREAD algorithm improves upon SPREAD by simultaneously accounting for both security and reliability requirements. The work in [2], [3] presents distributed Bound-Control and Lex-Control algorithms, which compute the multiple paths in such a way that the maximum performance degradation (e.g., throughput loss) is minimized when a single-link attack or a multi-link attack happens, respectively. The work in [6] considers the report fabrication attacks launched by compromised nodes. The work in further considers selective forwarding attacks, whereby a compromised node selectively drops packets to jeopardize data availability. Both works are based on a similar cryptographic method: the secret keys used by sensor nodes are specific to their geographic locations, which limits the impact of a compromised node. Instead of relying on a cryptographic method for resolving the issue, our work mainly exploits the routing functionality of the network to reduce the chance that a packet can be acquired by the adversary in the first place.

Given a set of paths that have been constructed, the third type of work studies the optimal way of using these paths to maximize security. For example, the Secure Message Transmission (SMT) mechanism proposed in [7] continuously updates the rating of the routes: For each successful (failed) share, the rating of the corresponding route is increased (decreased). The delivery of subsequent shares will be in favor of those routes with high ratings. The work in [1] studies two different ways of spreading an information packet into shares: secret sharing multi-path aggregation (SMA) and dispersed (message-splitting) multi-path aggregation (DMA). It shows SMA achieves better security at the cost of higher overhead, while the performance of DMA is exactly the complementary of SMA. In all above work, the multipath routing algorithms are deterministic in the sense that the same set of routes is always computed under the same topology. This weakness opens the door for a pin-pointed node-compromise or jamming attack, once the routing algorithm is acquired by the adversary.

b. Existing System

Existing randomized multi-path routing algorithms in WSNs have not been designed with security considerations in mind, largely due to their low energy efficiency. To the best of our knowledge, the work presented in this paper fills a void in the area of secure randomized multi-path routing. Specifically, flooding is the most common randomized multi-path routing mechanism. In flooding, every node in the network receives the packet and retransmits it once. To reduce unnecessary retransmissions and improve energy efficiency, the Gossiping algorithm was proposed as a form of controlled flooding, whereby a node retransmits packets according to a pre-assigned probability. It is well known that the Gossiping algorithm has a percolation behavior, in that for a given retransmission probability, either very few nodes receive the packet, or almost all nodes receive it. Parametric Gossiping was proposed in to overcome the percolation behavior by relating a node's retransmission probability to its hop count from either the destination or the source. A special form of Gossiping is the Wanderer algorithm, whereby a node retransmits the packet to one randomly picked neighbor. When used to counter compromised-node attacks, flooding, Gossiping, and parametric Gossiping algorithms actually help the adversary intercept the packet, because multiple copies of the same secret share are dispersed to many

nodes. The Wanderer algorithm has poor energy performance, because it results in long paths. In contrast, the NRRP, DRP, and MTRP schemes proposed in this paper are specifically tailored to security considerations in energy constrained WSNs. They provide highly dispersive random routes at low energy cost without generating extra copies of secret shares.

An information in the form of packets will be broken into several shares (M) i.e. components which carry partial information by using mechanisms such as threshold secret sharing mechanism. Here we can acquire the original information by combining the T shares, but not less than the T shares. But in this above approach, there will be several security related issues. The main problem is that this approach will not be better option if at all the adversary is capable of compromising or jamming the nodes. This is due to the fact that for the multiple routing algorithms, there will always be a fixed set of routes or paths. So once the adversary gets to know about the routing algorithm, the adversary can then calculate the group of routes for whichever of the specified source and destination [7]. During such circumstances, the challenger is able to pin-point to any of the one node and compromises those nodes. Secondly, since there will be only few no network machines-disjoint ways which could be established among source and destination. The main problem is that since the routes are calculated in some restrictions, the routes might not be spatially being dispersive enough for circumventing the black-hole [4].

c. Attacks on WSNs

Compromised Nodes - Node compromise occurs when an attacker, though some subvert means, gains control of a node in the network after deployment. Once in control of that node, the attacker can alter the node to listen to information in the network, input malicious data, cause DOS, black hole, or any one of a myriad of attacks on the network. The attacker may also simply extract information vital to the network's security such as routing protocols, data, and security keys. Generally compromise occurs once an attacker has found a node, and then directly connects the node to their computer via a wired connection of some sort. Once connected the attacker controls the node by extracting the data and/or putting new data or controls on that node.

Denial of Service - In computing, a denial-of-service (DoS) or distributed denial-of-service (DDoS) attack is an attempt to make a machine or network resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of efforts to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet.

Proposed System

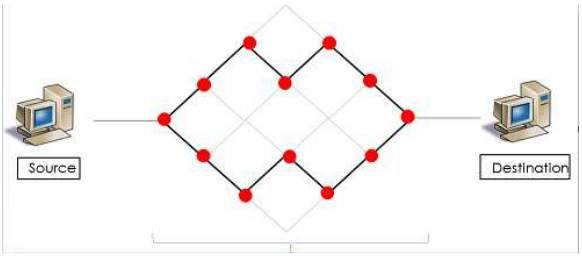

Figure :2 Proposed System.

Because of all the above mentioned problems, in this paper, we propose a randomized multipath routing algorithm which is capable of overcoming the above mentioned problems. The Existing system used to select pre-computed set of routes, but here the randomized multipath routing algorithm will create ways in an arbitrary mode every instance a packet requires to be sent. When it follows Randomized Multipath approach, the path changes whenever packet has to be sent. Because of this, a huge amount of routes will be created between every source and destination. The adversary, if it has to capture diverse packets, it may have to squash each and every potential routes through the source to the destination [6].

The proposed technique divides the information packets flowing through a single path to flow through two different paths and reach destination. By this approach when information will leave the source machine it will be split into 2 parts and take 2 different routes to reach destination machine. After reaching destination again the packets will be combined and presented to the user.

Study and analyses of information security problem while the Data is getting transmitted over a network helps to propose a technique that will solve most of the hacking problem by attackers.

a. Methodology

Here we propose a mechanism known as Secure Message Transmission (SMT) which will continuously update the rating of the routes which will be used to traverse. Whenever the transmission happens and if the corresponding route fails to transfer then rating will be decreased.

The energy consumption in case of proposed randomized multipath routing algorithms will be twice that of their deterministic counter parts. This algorithm could be useful to certain data packets in Wireless Sensor Networks to give extra safety against the attacker that try to get hold of the data packets.

ISSN: 2277-9655
Impact Factor: 1.852

Another feature of this algorithm is that by adjusting the secret sharing parameters as well as random propagation, diverse safety level could be offered at diverse power overheads. By taking into account the number of data packets that exists in WSNs, which requires low level of security, we can make sure that selective use of algorithm will not have a significant impact on the energy efficiency.

The proposed system which follows sensor technology is one with better, as well as cheaper technology which makes use of sensors which can be used both in civilian as well as military applications. This can mainly used in environments which is very harsh, unreliable or few times adversarial. Under such circumstances we deploy large number of sensors which helps in achieving high quality.

On another hand sensors mainly communicate with wireless sensor networks which have the network bandwidth less than wired communication. The above mentioned issues will bring new design to the DWSN (Distributed wireless Sensor Networks).

The proposed system which follows sensor technology is one with better, as well as cheaper technology which makes use of sensors which can be used both in civilian as well as military applications. On another hand sensors mainly communicate with wireless sensor networks which have the network bandwidth less than wired communication. The above mentioned issues will bring new design to the DWSN (Distributed wireless Sensor Networks).

Implemented Algorithm

The Algorithm proposed has the following three stages:

A. A Multipath Calculation algorithm to compute multiple paths.
B. A Multipath Forwarding algorithm to insure that packets travel on their specified paths.
C. An End-Host Protocol that effectively uses the determined multiple paths.

A. Path Algorithms

a) Generate paths based on desired characteristics of the path.
   – i.e. Maximized throughput or minimized delay
b) Generate Multi-Option paths and/or Multi-Service paths.
c) Path requirements depend on the end-user application.
   – i.e. Telnet vs. FTP
d) Two characteristics of a quality path:
   – Path Quantity
   – Path Independence
e) Some path algorithms that don't work:
   – Shortest K Paths, Link Disjoint Paths, Maximum Flow
f) Two path algorithms that do work:
   – Maximize Throughput: Capacity Removal
   – Minimize Latency: Discount Shortest Path
g) Both algorithms based on Dijkstra's Shortest Path algorithm.
h) Both algorithms produce shortest paths with minimal overlap by incrementally adding "cost" to each of the previously found paths

B. Path Forwarding

a) Path Forwarding Problem: how to specify a packets path and then forward packets along that path.
b) Each router has potentially multiple routes to a destination node.
c) The destination address is no longer sufficient.
d) A Path Identifier is now required for every packet.
e) Design Requirements for Path Forwarding:
   – Minimize Packet Overhead
   – Minimize router CPU overhead of forwarding packets
   – Minimize additional router memory

C. End-Host Protocol

a) Performance gains are only realized if end-hosts use the multiple paths effectively.
b) Paths can be used concurrently or one at a time.
c) The appropriate use of multiple paths is application specific.
   – Instant Messenger (multi-service)
   – Urgent Message (multi-option)

Multipath Routing Model

Multipath Routing Model consists of two different routing algorithms based on extensions of the traditional routing algorithms:
– MPDV (MultiPath Distance Vector)
– MPLS (MultiPath Link State)

Both routing algorithms seek to optimize throughput by using a Capacity Removal based algorithm and develop efficient path forwarding algorithms while minimizing packet and router overhead. This Model uses a fixed-length packet path ID to provide minimal packet overhead and allow efficient indexing into router forwarding tables.

A new transport layer called MPTCP (Multipath TCP) is created to ensure the safe transfer of the packets.

ISSN: 2277-9655
Impact Factor: 1.852

MPTC – Multi Path Transmission Control Protocol

MPTCP is based on single-path TCP and provides a reliable bit stream service. It operates by opening multiple TCP connections on different paths and then multiplexing data between them.

At the Destination, the receiving MPTCP layer collects data from each of the connections and then restores the original message stream. Un-interrupted data flow, congestion control are provided by MPTCP which increases network performance without any changes to user-applications. Simulated network is similar to the Internet topology with 100 nodes and 195 links across multiple clusters. Performance in such network is measured in throughput, latency, and message drop-off probability. Throughput is measured using MPTCP. Latency and drop-off probability is measured using multipath ping.

Of the various possible security threats encountered in a wireless sensor network (WSN), in this paper, we are specifically interested in combating two types of attacks: compromised node (CN) and denial of service (DOS).

In the CN attack, an adversary physically compromises a subset of nodes to eavesdrop information, whereas in the DOS attack, the adversary interferes with the normal operation of the network by actively disrupting, changing, or even paralyzing the functionality of a subset of nodes. These two attacks are similar in the sense that they both generate black holes: areas within which the adversary can either passively intercept or actively block information delivery. Due to the unattended nature of WSNs, adversaries can easily produce such black holes. Severe CN and DOS attacks can disrupt normal data delivery between sensor nodes and the sink, or even partition the topology.

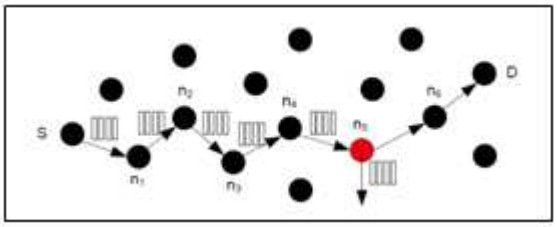

Figure 3 : Compromised Node Attack

A conventional cryptography-based security method cannot alone provide satisfactory solutions to these problems. This is because, by definition, once a node is compromised, the adversary can always acquire the encryption/decryption keys of that node, and thus can intercept any information passed through it. Likewise, an adversary can always perform DOS attacks (e.g., jamming) even if it does not have any knowledge of the underlying cryptosystem.

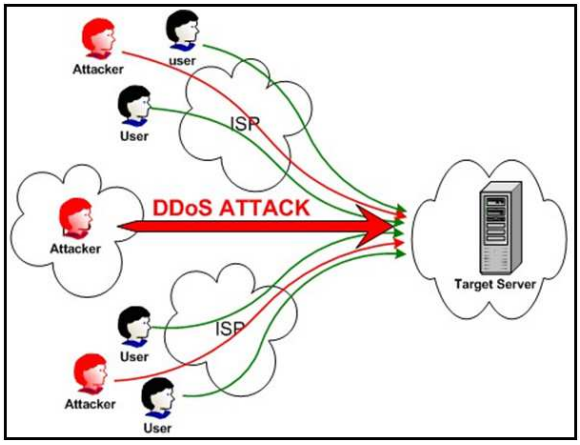

Figure 4: Denial of Service

Routing Algorithms

Routing algorithms generate paths that deliver messages from one vertex to another. One or multiple paths can be generated for the same pair of vertices. Multiple-path routing assures data redundancy, security, and integrity.

Test of Multiple paths

The student t-test might be used to test the result of multiple paths. However, we are still uncertain whether the pair success probability is equivalent to the pair connectivity. More attention is needed in this part.

Multipath consistency

This part needs more concern. We can validate that single path experimental results are consistent with the theory. But multipath results do not have a validation method yet. The relationship between the pair success probability and the pair connectivity ought to be discovered.

Energy Consumption

For wireless with limited energy supply, energy efficiency is important. Many energy saving mechanisms have been proposed previously. However, other than and, little research has been conducted to improve the energy efficiency of wireless networks through improved MAC contention resolution efficiency. Two-Phase BTPS achieves better energy efficiency than 802.11 due to significantly reduced collisions, in addition to the improved channel utilization and the packet access delay. To measure the energy consumption of mobile stations, we assume the power consumption model of

2.4 GHz DSSS Lucent IEEE 802.11 WaveLAN PC Card operating in ad-hoc mode with channel bit rate of 11 Mbps.

The evaluation metric, access energy cost, is defined as the total energy consumed by all stations divided by the aggregate throughput. As each contending station is constantly backlogged, the more the contending stations, the longer (on average) a station has to wait before transmitting a packet. Hence, the access energy cost naturally increases with the number of the contending stations, which can be observed for both 802.11 and Two-Phase BTPS. However, as a station consumes more energy in the transmission mode than in other modes, a MAC protocol suffering more collisions will be less energy-efficient. The difference between Two-Phase BTPS and 802.11 in RTS retransmissions leads to the difference in energy consumption, which explains why the access energy cost of 802.11 degrades much faster than Two- Phase BTPS with the increase of the contending stations.

Random Multi Path Routing Algorithm

Purely Random Propagation Routing (PRP)

To diversify routes, an ideal random propagation algorithm would propagate shares as dispersive as possible. Typically, this means propagating the shares farther from their source. At the same time, it is highly desirable to have an energy-efficient propagation, which calls for limiting the number of randomly propagated hops. A share may be sent one hop farther from its source in a given step, but may be sent back closer to the source in the next step, wasting both steps from a security standpoint.

To tackle this issue, some control needs to be imposed on the random propagation process. In PRP, shares are propagated based on one-hop neighborhood information. More specifically, a sensor node maintains a neighbor list, which contains the ids of all nodes within its transmission range. When a source node wants to send shares to the sink, it includes a TTL of initial value N in each share. It then randomly selects a neighbor for each share, and unicasts the share to that neighbor. After receiving the share, the neighbor first decrements the TTL. If the new TTL is greater than 0, the neighbor randomly picks a node from its neighbor list (this node cannot be the source node) and relays the share to it, and so on. When the TTL reaches 0, the final node receiving this share stops the random propagation of this share, and starts routing it toward the sink using normal min-hop routing. The WANDERER scheme is a special case of PRP with N 1/41. The main drawback of PRP is that its propagation efficiency can be low, because a share may be propagated back and forth multiple times between neighboring hops.

Non repetitive Random Propagation (NRRP)

NRRP is based on PRP, but it improves the propagation Efficiency by recording the nodes traversed so far. Specifically, NRRP adds a “node-in-route” (NIR) field to the header of each share. Initially, this field is empty. Starting from the source node, whenever a node propagates the share to the next hop, the id of the upstream node is appended to the NIR field. Nodes included in NIR are excluded from the random pick at the next hop. This non repetitive propagation guarantees that the share will be relayed to a different node in each step of random propagation, leading to better propagation efficiency.

Directed Random Propagation (DRP)

DRP improves the propagation efficiency by using two hop neighborhood information. More specifically, DRP adds a “last-hop neighbor list” (LHNL) field to the header of each share. Before a share is propagated to the next node, the relaying node first updates the LHNL field with its neighbor list. When the next node receives the share, it compares the LHNL field against its own neighbor list, and randomly picks one node from its neighbors that are not in the LHNL. It then decrements the TTL value, updates the LHNL field, and relays the share to the next hop, and so on. Whenever the LHNL fully overlaps with or contains the relaying node’s neighbor list, a random neighbor is selected, just as in the case of the PRP scheme According to this propagation method, DRP reduces the chance of propagating a share back and forth by eliminating this type of propagation within any two consecutive steps. Compared with PRP, DRP attempts to push a share outward away from the source, and thus, leads to better propagation efficiency for a given TTL value.

Data Splitting that is performed based on packet happens at the source only, not in internal Nodes. If the total channel packet rate is assumed to be 11 Mbps, the data that is split can be transmitted over a Size of 400m×400m and Range of 40m Nodes: 300, 400, 500, 600, 700, 800, and 900.

The bandwidth division between the control and the data channels causes the number of contending stations and the average data packet size all determine T1 and T2, the performance of DCPS varies with various network parameters.

Selection of Path:

Routing is the process of selecting best paths in a network. In the past, the term routing was also used to mean forwarding network traffic among networks. However this latter function is much better

ISSN: 2277-9655
Impact Factor: 1.852

described as simply forwarding. New route selection mechanisms for MANET routing protocols, which we call the minimum drain rate (MDR) and the conditional minimum drain rate (CMDR). MDR extends nodal battery life and the duration of paths, while CMDR also minimizes the total transmission energy consumed per packet. Using the ns-2 simulator and the dynamic source routing (DSR) protocol, we compare MDR and CMDR against prior proposals for energy-aware routing and show that using the drain rate for energy-aware route selection offers superior performance results. Methods keywords are system design and simulations.

Distance vector algorithms

Distance-vector routing protocol

Distance vector algorithms use the Bellman–Ford algorithm. This approach assigns a *cost* number to each of the links between each node in the network. Nodes will send information from point A to point B via the path that results in the lowest *total cost* (i.e. the sum of the costs of the links between the nodes used). The algorithm operates in a very simple manner. When a node first starts, it only knows of its immediate neighbors, and the direct cost involved in reaching them. (This information the list of destinations, the total cost to each, and the *next hop* to send data to get there makes up the routing table, or *distance table*.) Each node, on a regular basis, sends to each neighbor node its own current assessment of the total cost to get to all the destinations it knows of. The neighboring nodes examine this information and compare it to what they already 'know'; anything that represents an improvement on what they already have, they insert in their own routing table(s). Over time, all the nodes in the network will discover the best next hop for all destinations, and the best total cost.

When one network node goes down, any nodes that used it as their next hop discard the entry, and create new routing-table information. These nodes convey the updated routing information to all adjacent nodes, which in turn repeat the process. Eventually all the nodes in the network receive the updates, and discover new paths to all the destinations they can still "reach". e.g. RIPV1, RIPV2

Link-state algorithms

Link-state routing protocol

When applying link-state algorithms, a graphical map of the network is the fundamental data used for each node. To produce its map, each node floods the entire network with information about the other nodes it can connect to. Each node then independently assembles this information into a map.

Using this map, each router independently determines the least-cost path from itself to every other node using a standard shortest paths algorithm such as Dijkstra's algorithm. The result is a tree graph rooted at the current node, such that the path through the tree from the root to any other node is the least-cost path to that node. This tree then serves to construct the routing table, which specifies the best next hop to get from the current node to any other node.

Optimized Link State routing algorithm

Optimized Link State Routing Protocol

A link-state routing algorithm optimized for mobile ad hoc networks is the *Optimized Link State Routing Protocol (OLSR)*. OLSR is proactive; it uses Hello and Topology Control (TC) messages to discover and disseminate link state information through the mobile ad hoc network. Using Hello messages, each node discovers 2-hop neighbor information and elects a set of *multipoint relays*(MPRs). MPRs distinguish OLSR from other link state routing protocols.

Dijikstra's Algorithm

Illustration of Dijkstra's algorithm search for finding path from a start node (lower left, red) to a goal node (upper right, green) in a robot motion planning problem. Open nodes represent the "tentative" set. Filled nodes are visited ones, with color representing the distance: the greener, the farther. Nodes in all the different directions are explored uniformly, appearing as a more-or-less circular wave front as Dijkstra's algorithm uses a heuristic identically equal to 0. Let the node at which we are starting be called the initial node. Let the distance of node *Y* be the distance from the initial node to *Y*. Dijkstra's algorithm will assign some initial distance values and will try to improve them step by step.

1. Assign to every node a tentative distance value: set it to zero for our initial node and to infinity for all other nodes.
2. Mark all nodes unvisited. Set the initial node as current. Create a set of the unvisited nodes called the *unvisited set* consisting of all the nodes.
3. For the current node, consider all of its unvisited neighbors and calculate their *tentative* distances. For example, if the current node *A* is marked with a distance of 6, and the edge connecting it with a neighbor *B* has length 2, then the distance to *B* (through *A*) will be 6 + 2 = 8.
4. When we are done considering all of the neighbors of the current node, mark the current node as visited and remove it from the *unvisited set*. A visited node will never be checked again.

5. If the destination node has been marked visited (when planning a route between two specific nodes) or if the smallest tentative distance among the nodes in the *unvisited set* is infinity (when planning a complete traversal; occurs when there is no connection between the initial node and remaining unvisited nodes), then stop. The algorithm has finished.
6. Select the unvisited node that is marked with the smallest tentative distance, and set it as the new "current node" then go back to step 3.

Our analysis and simulation results have shown the effectiveness of the randomized dispersive routing in combating CN and DOS attacks. By appropriately setting the secret sharing and propagation parameters, the packet interception probability can be easily reduced by the proposed algorithm which is at least one order of magnitude smaller than approaches that use deterministic node-disjoint multipath routing. From the simulation results one can conclude that in PRP routing algorithm is less efficient because the packet can transverse back and forth. In NRRP the dispersive routes will avoid back and forth propagation because of NIR field's storage. DRP routing algorithm works even better because of comparison of two LHNL fields.

Conclusion

The Randomized Multi-Path Routing Algorithm proposed in this paper aims to provide a secure and robust way of Data Transmission. The Robustness of the Algorithm is based on the concept of path rating. The Random path selected for the data transmission is given a high rating if the data packet is delivered securely. Based on the Rating the data is split and sent on routes with higher rating to achieve high amount of Successful Data Transmission. The Data arriving at the Receiver is combined and made available to the user.

The advantage of this technique would be, in case if any of the path get hack the attacker will never get to know the exact information as it would be partial. The System elaborates the design of the randomized multi-path routing mechanism and analyzes the performance of the baseline PRP scheme.

References

[1] *Ross. A, (2001), "Security Engineering: A Guide to Building Dependable Distributed Systems", New York: John Wiley & Sons, Inc.*

[2] *Barrett.C. L, Eidenbenz.S. J, Kroc.L, Marathe.M and Smith.J. P (2003) "Parametric probabilistic sensor network routing", In Proceedings of the ACM International Conference on Wireless Sensor Networks and Applications (WSNA), pp. 122–131.*

[3] *Johnson.D. B, Maltz.D. A, and Broch.J (2001), "DSR: The dynamic source routing protocol for multihop wireless ad hoc networks" In C. E. Perkins, editor, Ad Hoc Networking,Addison-Wesley. pp. 139–172.*

[4] *Li.X. Y, Moaveninejad.K, and Frieder.O, (Feb. 2005), "Regional gossip routing wireless ad hoc networks", ACM Journal of Mobile Networks and Applications, Volume 10, no.(1-2), pp.61–77.*

[5] *Lou.W, Liu.W and Zhang.Y, (2006), "Performance optimization using multipath routing in mobile ad hoc and wireless sensor networks", In Combinatorial Optimization in Communication Networks, pp. 117–146.*

[6] *Mavropodi.R, Kotzanikolaou.P and Douligeris.C, (Jan. 2007) "Secmr - A secure multipath routing protocol for ad hoc networks", Elsevier Journal of Ad Hoc Networks, Volume 5, no.1, pp.87–99.*

[7] *Marina.M. K and Das.S. R, (Nov. 2001), "On-demand multipath distance vector routing in ad hoc networks", In Proceedings of the IEEE International Conference for Network Protocols (ICNP), pp. 14–23.*