Volume 5, Issue 9, September 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Defending Wireless Sensor Network using Randomized Routing

R. Jegadeesan
Assistant Professor (CSE)
R.M.K .Engineering College, Chennai, India

N. Sankarram
Professor & Head (CSE)
R.M.K .College of Engg and Technology, Chennai, India

Abstract: Wireless Sensor Network (WSN) challenges in the transmission of data are its network traffic and network security. Another issue in sensor network is Compromised node and Denial -of -service attack (DOS).Multipath Routing Algorithms are vulnerable to these attacks. A Key Management scheme is used with this routing algorithm to generate randomized multipath routes for secure transmission of data to the sink. We adopt Shamir's algorithm for efficient key management which is scalable, highly secure and decreases communication overhead. Randomized Route Generation changes the routes taken by the shares from time to time thereby increasing the probability of randomness of paths to be selected for transferring data in a much secured manner.

To bypass the black hole, opponent has to selectively compromise nodes or block the shares containing the message which traverse randomly which is very difficult.

Keywords - (NRRP), Directed Wireless sensor network (WSN), Purely Random Propagation (PRP), Non-Repetitive Random Propagation Random Propagation(DRP) , Multicast Tree Random Propagation(MTRP).

I. INTRODUCTION

In WSN, number of protocols and routing algorithms have been proposed for resource-limited secured data transfer. Although fundamental notations of WSN research are well established, optimization of the limited resources has motivated new research directions in the field. In this paper, we seek to present general principles to aid in the design of secure WSN multipath routing using randomized route Generation. Therefore, we have to establish new concepts, envisioned applications, and the experience garnered from the WSNs research, we first review the desired security services and topology construction (i.e., confidentiality, authentication, integrity, access control, availability, and no repudiation) from WSNs perspective. Then, we review which routing algorithm would be necessary for resource-constrained WSNs and how it defends the Wireless Sensor Network attacks. repudiation) from WSNs perspective. Then, we review which routing algorithm would be necessary for resource-constrained WSNs and how it defends the Wireless Sensor Network attacks.

In this paper, we defend attacks in Wireless Sensor Network by constructing topology bypass scheme and evaluating the multipath routes to increase security. Here nodes are dynamic, the topology construction is based on mesh topology. WSN Threats comprised of Member attacks which is of authenticated member and non-authenticated member. Method Specific attacks such as active attack (dynamic one) and passive attack (attack which occurs slowly in static).Target Specific attacks such as sink node attack, source node attack, neighbor attack.

A mesh network can be designed using a flooding technique or a routing technique. When using a routing technique, the message is propagated along a path, by hopping from node to node until the destination is reached. To ensure all its path availability, a routing network must allow for continuous connections and reconfiguration around broken or blocked paths, using self-healing algorithms. A mesh network whose nodes are all connected to each other is a fully connected network.

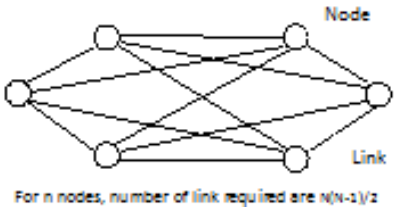
II. PROBLEM ANALYZATION

1. TOPOLOGY CONSTRUCTION USING MESH TOPOLOGY

Mesh topology is constructed because of unstructured nature. Topology is constructed by having node name and connections among the nodes as input from user , the port number and IP address is also obtained while adding next node , comparison of nodes will be done to avoid node duplication

The gateways and nodes work together to form a mesh network. The gateway maintains a list of nodes (by serial number) that have been authorized for network access. When a node powers up, it scans for available networks, locates either a gateway or router, and attempts to join it. If the gateway has the node in its list, the node joins the network, downloads the latest configuration from the gateway, and begins its normal operation of acquiring measurement data and controlling DIO. Since each node joins a network instead of a particular router or gateway, it can find a new path back to the gateway in the event that the signal is lost or blocked to its existing network route. In this way, the mesh network is inherently self-forming and self-healing. However, this may also cause network throughput to decrease, as there is no way to force a router or end node to join to a particular device in the network. Each time a node joins through a router, the overall throughput of that node is halved, due to the fact that the node must hop to get its messages back to the gateway.

DIAGRAM OF TOPOLOGY CONSTRUCTION USING MESH NETWORK



Our goal is to design a distributed random route for the shares which selects the best data allocation path across multiple paths through a probabilistic nature. This enhances the traditional centralized solution since the end user need not have thorough knowledge about network topology, therefore we can have it for all systems which is been decentralized and even the sensor nodes is been in different domains and handled independently. Our primary security intent is to minimize the maximum damage incurred by attacks and to increase network security, decrease network loss, increase flexibility when examining it with centralized approach.

Our primary security intent is to minimize the maximum damage incurred by attacks and to increase network security, decrease network loss, increase flexibility when examining it with centralized approach. According to our simulation, we examine the security of randomized routing against different types of attacks on nodes/links. This algorithm reduces the security cost and retransmission is avoided by using suitable propagation phase depending upon short route using Dijkstras algorithm. In our simulation, we use Location-based protocols ,Data Centric Protocols , Multipath - based Protocols , QoS-based Protocols.

Randomized routing Algorithm is the best multipath routing algorithm where the route is been selected dynamically from a random time constraint among the probabilistic one. Randomized routing Algorithm have the four principles: Purely Random Propagation (PRP), Non-Repetitive Random Propagation (NRRP), Directed Random Propagation (DRP), Multicast Tree Random Propagation (MTRP)

2. KEY MANAGEMENT OF RSA ALGORITHM

The RSA algorithm involves three steps: key generation, encryption and decryption.

Key Generation:

Compute n = pq.

n is used as the modulus for both the public and private keys. Its length, usually expressed in bits, is the key length.

Compute $\varphi(n) = \varphi(p)\varphi(q) = (p - 1)(q - 1)$, where φ is Euler's function. RSA involves a public key and a private key. The public key can be known by everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted in a reasonable amount of time using the private key. The keys for the RSA algorithm are generated the following way:

Choose two distinct prime numbers p and q. For security purposes, the integer's p and q should be chosen at random, and should be of similar bit-length. Prime integers can be efficiently found using a primality test.

Choose an integer e such that $1 < e < \varphi(n)$ and $\gcd(e,\varphi(n)) = 1$; i.e., e and φ(n) are co prime.

e is released as the public key exponent.

e having a short bit-length and small Hamming weight results in more efficient encryption – most commonly 216 + 1 = 65,537. However, much smaller values of e (such as 3) have been shown to be less secure in some settings.[5]

Determine d as $d \equiv e^{-1} \pmod{\varphi(n)}$; i.e., d is the multiplicative inverse of e (modulo φ(n)). This is more clearly stated as: solve for d given $d \cdot e \equiv 1 \pmod{\varphi(n)}$

This is often computed using the extended Euclidean algorithm. Using the pseudo code in the Modular integers section, inputs a and n correspond to e and φ(n), respectively. d is kept as the private key exponent.

The public key consists of the modulus n and the public (or encryption) exponent e. The private key consists of the modulus n and the private (or decryption) exponent d, which must be kept secret. p, q, and φ(n) must also be kept secret because they can be used to calculate d.

An alternative, used by PKCS#1, is to choose d matching $de \equiv 1 \pmod{\lambda}$ with $\lambda = \operatorname{lcm}(p - 1, q - 1)$, where lcm is the least common multiple. Using λ instead of φ(n) allows more choices for d. λ can also be defined using the Carmichael function, λ(n).

The ANSI X9.31 standard prescribes, IEEE 1363 describes, and PKCS#1 allows, that p and q match additional requirements: being strong primes, and being different enough that Fermat factorization fails.

Encryption

Alice transmits her public key (n, e) to Bob and keeps the private key secret. Bob then wishes to send message M to Alice. He first turns M into an integer m, such that $0 \leq m < n$ by using an agreed-upon reversible protocol known as a padding scheme. He then computes the cipher text c corresponding to c=equivalent of m^e \ p mod{n}

This can be done quickly using the method of exponentiation by squaring. Bob then transmits c to Alice.

Note that at least nine values of m will yield a cipher text c equal to m, but this is very unlikely to occur in practice.

Decryption

Alice can recover m from c by using her private key exponent d via computing m \equiv c^d \pmod{n}

Given m, she can recover the original message M by reversing the padding scheme. (In practice, there are more efficient methods of calculating c, d using the recomputed values.

3. REQUIREMENT OF KEY MANAGEMENT

- Confidentiality- Nodes should not reveal data to any unintended recipients.
- Integrity- Data should not be changed between transmissions due to environment or malicious activity.
- Data Freshness- Old data should not be used as new.
- Authentication- Data used in decision making process should originate from correct source.
- Robustness- When some nodes are compromised the entire network should not be compromised.
- Self-organization- Nodes should be flexible enough to be self-organizing (autonomous) and self-healing (failure tolerant).
- Availability- Network should not fail frequently

III. ROUTING MODEL

Wireless sensor network is spatial layered networks which do not have infrastructure and layered network communication or transferring of data is done through nodes which can be done through one hop or multi hop based on the selected propagative routing algorithm.

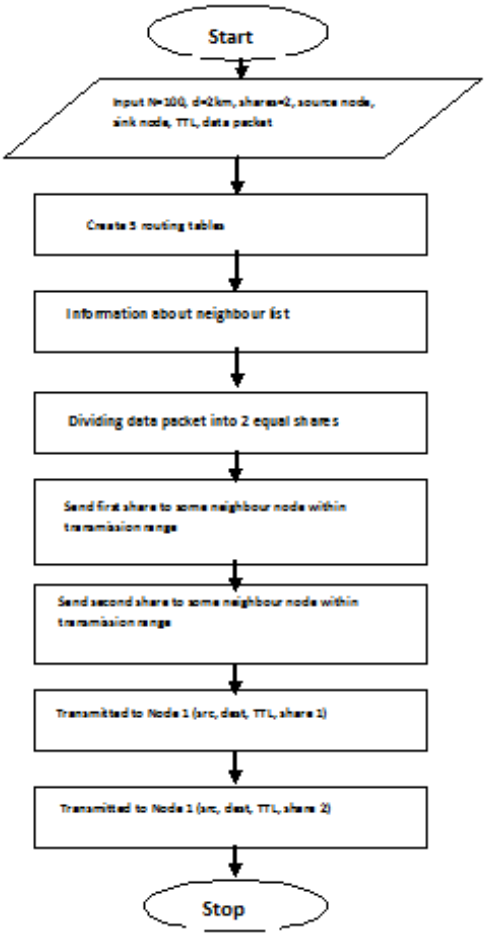
All wireless sensor nodes are battery operated and lifetime of network depends on the battery power available to a node. After transmitting a data, the battery bower of the node might reach to a threshold value. The data transmission range is not fixed; it changes to different area of different node. The randomized multipath delivery has 3-phase such as:

- sharing of data secretly by having key management.
- by having randomized propagation.
- by having min–hop routing toward link.

1. PRP

In this propagation phase, one –hop neighborhood information, a sensor node has a neighbor list, which include the id's of all nodes in its area of transmission. While data transmission, when a source node has to send shares to sink node, it includes a TTL value of initial value n in each end every share. It selects a neighbor randomly for each share and cast the share in a single direction, when the share is been received by sink node, TTL value is been decremented first ,if the new TTL>o, the neighbor picks a node from neighbor list and propagate the share to it .when TTL =0, the random propagation of this share is stopped, and start routing toward the sink using min –hop routing. The WANDERER scheme is a pure random-walk algorithm in PRP. The drawback of PRP is that of low propagation efficiency, since it can travel back and forth between neighboring nodes

Flowchart of PRP describes about dividing packets into shares and transmitting them over randomly dispersed route.



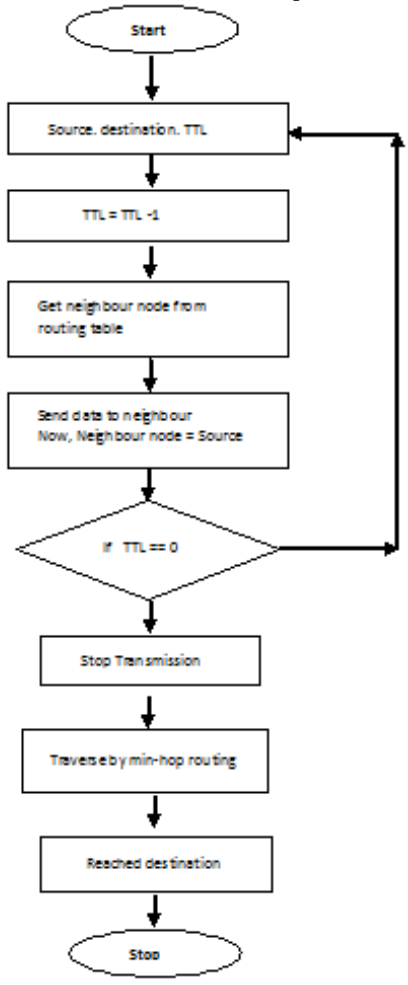
Flow Chart representing PRP phase

2. NRRP

NRRP is same as of PRP, but it has improved propagation efficiency by having NIR field which record and store about the nodes traversed so far, NRRP has NIR field in the header of each share. Initially, this field is empty and when node propagates the share to next hop of node from source node, the id of upstream node is recorded to the NIR field. Node recorded in NIR is then excluded from random pick at the next hop. So, a node which traverse in a path cannot be transmitted or traversed in the same path again and again which avoid retransmission and leads to a better propagation efficiency.

3. DIRECT RANDOM PROPAGATION (DRP)

DRP occurs by using two hop neighborhood information. DRP adds a LHNL field which is the last hop neighbor list field to the header of each share which propagates to the next node , it checks with the LHNL field against its own neighbor list ,and transmit by random picking of node only if it is not in neighbor list ,then TTL value is decremented , and so on Mesh topology is constructed because of unstructured nature. Topology is constructed by having node name and connections among the nodes as input from user , the port number and IP address is also obtained while adding next node , comparison of nodes will be done to avoid node duplication.



4. MULTICAST TREE RANDOM PROPAGATION

MTTP has directionality , the most energy efficient since it has the end –to –end shortest path which is geographically distributed and the share propagate towards sink direction, this routing requires location information of nodes , intermediate nodes . GPSR and LAR are Example of location – based routing which has MTRP phase relies on GPS in each node or on some distributed localization algorithm. Under MTRP, the header of each share , have two fields max^{hop} and min^{hop}.

$max^{hop} = ns+\infty 1$

$min^{hop} = ns-\infty 2$

Where,

Ns□hop count from source to sink

∞1,∞2□-non-negative integers

∞1□propagate away from the sink i.e,left half of circle.

∞2□propagate towards the sink i.e,right half of circle

Filters node that have hop count greater than max hop or smaller than min hop , the next relaying node is choosed randomly from remaining neighbors

Drawbacks

High cost, low accuracy of localization. Filters node that have operation count greater than max hop or smaller than min hop , the next relaying node is chosen randomly from remaining neighbors.

IV. CONCLUSION

Our simulation result shows the efficient transmission of data using randomized multipath routing which defends Wireless Sensor Network Attacks. The packet interception is been reduced by having secret sharing mechanism(T,M)and properly having secret key and propagation phase and from our simulation we can verify that security cost and interception of packet is reduced .Retransmission occurs less so that communication overhead is reduced thereby resulting in decrease of server overload. The proposed algorithms can be applied to selective packets in network transmission range to offer additional security levels against adversaries attacking underlying cryptography system.

PRP is less efficient since the packet can traverse forward and backward, but in NRRP, MTRP these drawbacks can be avoided since they have node in route fields which stores all the traverse records, and DRP too have its efficiency since it has the last hop node list which will be our future study work.

REFERENCES

[1] Nicolas Gouvy,Essia hamouda,Nathalie Mitton and Dimitrios Zorbas,"Energy Efficient Multi-Flow Routing in Mobile Sensor Networks,"IEEE Conference ,2013 (8)

[2] W. Lou and Y.Kwon . H-SPREAD : A Hybrid Multipath scheme for secure and reliable data collection in wireless sensor networks, IEEE Transactions on Vehicular Technology , 55(4):1320-1330,July 2006

[3] P.Karunakaran and Dr. C. Venkatesh,"Traffic and Security using Randomized Dispersive Routes in Heterogeneous Sensor Network," IJDPS vol3.No.1,2012

[4] Anfeng Liu, Zhongming Zheng, Chao Zhang, Zhigang Chen and Xuemin Shen,"Secure and Energy-Efficient Disjoint Multipath Routing for WSNs,"IEEE Transactions on Vehicular Technology, vol 51.No 7,2012

[5] Lei wang , Yuwang Yang and Wei Zhao, " Network coding-based multipath routing for energy efficiency in Wireless Sensor Networks,"EURASIP Journal on Wireless Communication and Networking , 2012.

[6] Daojing He,Sammy Chan , Shaohua Tang , and Mohsen Guizani,"Secure Data Discovery and Dissemination based on Hash Tree for Wireless Sensor Networks,"IEEE Transactions on Wireless Communications,Vol.12,No.9,2013

[7] Huang Lu,Jie Li,Mohsen Guizani,"Secure and Efficient Data Transmission for Cluster-based Wireless Sensor Networks,"IEEE Transactions on Parallel Distributed Systems, 2012

