www.ijecs.in
International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 5 Issue 1 Dec 2016, Page No. 15421-15427

Enhanced Security In Data Transmission In Wireless Sensor Network Using Randomized Path

***M Uma*[1], *Dr. A Senthil Kumar*[2]**
[1]*Research Scholar, Bharathiar University.* Tamilnadu
[2]*Assistant professor. Department of Computer Science, Govt. Arts college* Namakkal

Abstract: The one of the most important application for gathering specific information from the surrounding environment is WSN, so it is important to safeguard the sensitive data from unauthorized access. The security level in the WSN against the attacks in susceptible due to broadcast. There are two key attacks in WSN such as compromised node and denial of service.The key attack Compromised node(CN) attack which has the ability to create black hole, thereby interrupting the active information delivery and denial of service attack in attempt to make a network resource unavailable to its intended users, such as to temporarily or indefinitely interrupt or suspend services. In this paper we advance the mechanism that generate randomized multipath routes. In this mechanism that generate randomized multipath routes that means shares of different packets change over time. Incase the adversary came to know the routing algorithm,but it can't identify the routes traversed by each packet more over randomness, the generated routes are also highly dispersive and energy efficient making them quite capable of bypass the black holes.

Key words :Security , Compromised node , Denial of Service, Randomized route.

2. INTRODUCTION

2.1 Security Necessities Of Common Wireless Network

A WSN comprises of a enormous number of sensornodes. They are arranged over an range and process awireless network. Therefore, WSNs also comprisewireless network's security requirements. Thesolutions against susceptibility of common wirelesssystem are précised as follows:

- **Authentication:** Authentication is theprocedure of put off whether someone orsomething is, in fact, who or what they haveacknowledged to be in wireless commutations[2].

- **Confidentiality:** Assurance that informationis pooled only among approved persons orsystems with wireless networks[2].

- **Integrity**: Assurance that the information istrustworthy and complete in wireless communications

- **Non Repudiation**: All parties to a transactionmust be confident that the transaction isprotected. The system must ensure that a party Cannot subsequently reject a inwireless communication transaction[2].

Existing System

SPREAD algorithm in goes to find multiple most-secure and node-disjoint paths. Thesecurity of a path is defined as the probability of node compromise along that path, and is labeledas the weight in path collection. [3][5]A modified Dijkstra algorithm is used to iteratively find the top-K most secure node-disjoint paths. The H-SPREAD algorithm improves upon SPREAD bysimultaneously bookkeeping for both security and consistency requirements Distributed Bound-Control and Lex-Control algorithms, which computes multiple paths, respectively, in such a waythat the appearance degradation (e.g., throughput loss) is minimized when a single-link attackor a multi-link attack occurs, respectively

Flooding is the most common randomized multipath routing mechanism. As a result, every node in the network receives the packet andretransmits it once. To reduce unnecessary retransmissions and improve energy efficiency, theGossiping algorithm was proposed as a form of controlled flooding, whereby a node retransmitspackets according to a pre-assigned probability[3].Parametric Gossiping was proposed in to overcome the percolation behavior by relating anode's retransmission probability to its hop count from either the destination or the source. Aspecial form of Gossiping is the Wanderer algorithm, whereby a node retransmits the packet toone randomly picked neighbor. When used to counter compromised-node attacks, flooding, Gossiping, and parametric Gossiping actually help the adversary intercept the packet, because multiple copies of a secret share are dispersed to many nodes.[3][5]

Disadvantages of 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[4].

Multi-path routing mechanism, Gossiping algorithm has a percolation behavior, in thatfor a given retransmission probability, either very few nodes receive the packet, or almostall nodes receive it.

The Wanderer algorithm has poor energy performance, because it results in long paths

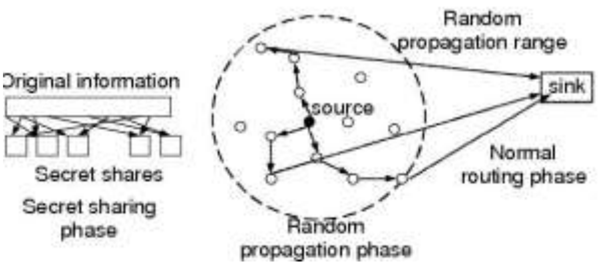
WIRELESS SENSOR NETWORK

Due to the unattended environment ofWSNs, adversaries can certainly produce such black holes.Simple CN and DOS attacks can interruptregular data delivery sandwiched between sensor nodes and the sink, or even divider thetopology.[5] A conservative cryptography-based security method cannot alone provide satisfactory solutions to these problems. This is because, by definition, once a node is bargained, the adversary can always get the encryption/decryption keys of that node, and thus can capture any information passed through it. At the same time, an adversary can always perform certain form of DOS attack (e.g., jamming) even if it does not have any awareness of the crypto-system used in the WSN. To bypass the black holes the premature time's idea is implemented in a probabilistic manner, typically through a two-step process: secret sharing and multi-path routing. First, an data (e.g., a packet) is Broken into *M segments*(i.e., components of a packet that carry part information) using a ($T:M$)-threshold secret-sharing mechanism such as the Shamir's algorithm. The originalinformation can be recovered from a blend of at least$T$ segments, but no information can be deduced from less than Tsegments. Then, multiple routes from the source to the destinationare calculatedaccording to some multi-path routing algorithm. The$M$ shares are then distributed across theseroutes and delivered to the destination, following differentpaths. As long as at least M ¡T +1 (or T) shares bypass thecompromised nodes, the adversary cannot acquire the original information packet, but three security problem occurs in the above counter attacks first, approach is no longer validif the adversary can *selectively* compromise or jam nodes.This is because the route computation in the above multipathrouting algorithms is deterministic in the intelligence that fora fixed topology, a fixed set of routes are always computedby the routing algorithm for given source and destination.Therefore, even if the shares can be spread over differentroutes, overall they are always delivered over the same setof routes that are calculable by the algorithm. As aoutcome,once the routing algorithm becomes open to the adversary(this can be done through a memory interrogation of thecompromised nodes), the adversary can by itself compute theset of routes for any given source and destination. Second Infactvery few node-disjoint routes can be found when node densityis adequate and source and destination nodes are several stagesapart. The absence of sufficient routessuggestively weakens the security performance of this multipathapproach. Third, the set of routesis computed under certain constraints, the routes may not bespatially dispersive enough to circumvent a moderate-sizedblack hole. In this paper, we put forward a randomized multi-path routing algorithm that can stunned the above problems.[6] As an alternative of picking paths from a pre-computed set of routes, this algorithm calculates multiple paths in a randomized technique eachtime an information packet needs to be sent, such that the set of routes taken by various shares of different packets keep changing over time.[7] As a result, a large number of routes canbe possibly generated for each source and destination. To interrupt different packets, the adversary has to negotiationor jam all likely routes from the source to the destination,which is basically infeasible.

3. RANDOMIZED MULTI-PATH DELIVERY

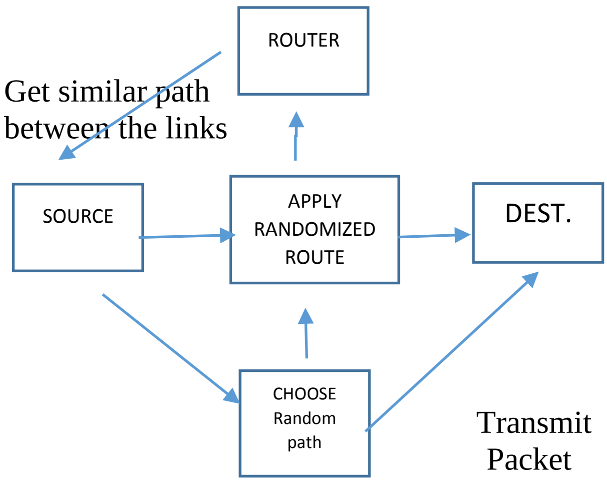
3.1 RANDOMIZED ROUTE

As explained in Figure 1, we consider a 3-phase approach for secure information delivery in a



WSN: secret sharingof information, randomized propagation of each informationshare, and normal routing (e.g., min-hop routing) toward the Sink. More precisely, when a sensor node needs to direct apacket to the sink, it first breaks the packet into *M* sharesaccording to a (*T;M*)-threshold secret sharing algorithm, e.g., the Shamir's algorithm . Every share is then transferred toparticular randomly picked neighbor. That neighbor will carry onto communicate the share it has received to other randomly selected neighbors, and so on. In each information share, there is a TTLfield, whose opening value is set by the source node to control the total number of randomized relays. After each relay, theTTL field is reduced by 1. When the TTL count reaches 0, thefinal node receiving this share stops the random propagationphase and begins to route this share in the direction of the sink usingnormal single-path routing. Once the sink collects at least *T*shares, it can inversely compute the original information. Noinformation can be recuperated from less than *T* shares.Because routes are randomly generated, there is no guaranteethat different routes are still node-disjoint. However,the algorithm should ensure that the randomly generatedroutes are as dispersive as possible,[8] i.e., different routes are in nature separated as far as possible such that theyhave high chances of not simultaneously passing through ablack hole. Considering the stringent requirement on energyconsumptions in WSNs, the major challenge in our designis to generate highly dispersive random routes at low energycost.Atrusting algorithm of generating random routes, such as Wandererscheme (a pure random-walk algorithm), only indications tolong paths (containing many hops, and therefore, consumingmuch energy) without accomplishing good dispersiveness. Due tosecurity considerations, we also necessitate that the route calculationbe applied in a distributed way, such that thefinal route signifies the aggregate choice of all the nodesparticipating in route selection. As a result, a small numberof colluding/compromised nodes cannot control the selectionresult. In addition, for efficiency purposes, we also require thatthe randomized route selection algorithm only acquires a smallamount of communication overhead. Unnecessary to say, the random propagation phase is the keycomponent that dictates the security and energy performanceof the entire mechanism. We further elaborate on the designof this module in the following subdivisions.[6][7]

Routing Mechanism



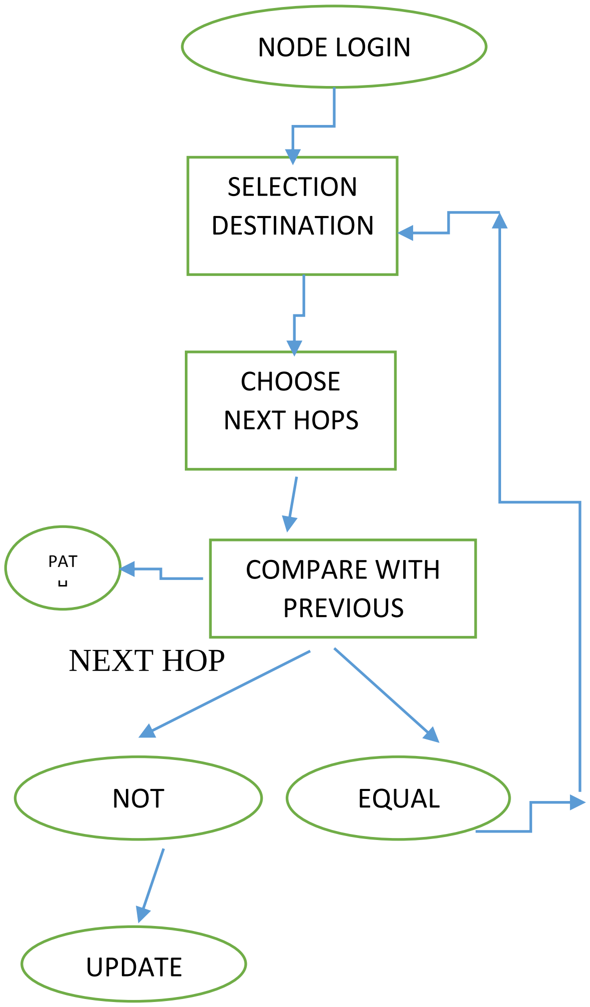
SELECT RANDOM PATH

The following diagram shows how the rondom routes are selected in the networks

Here multiple paths are computed in a randomized way eachtime an information packet needs to be sent, such that the set of routes taken by various shares ofdifferent packets. And path are selected by the comparison table in the path. .[6][7]

Depending on the type of data that has to be sent from the node, there are four randomized dispersive routing mechanisms have been developed by Tuo Shu et. Al . They are Purely Random Propagation (PRP); Non Repetitive Random Propagation (NRRP); Directed Random Propagation (DRP) ;

Multi cast Tree -assisted Random Propagation (MTRP). These methods differ in the way they choose their next node while traversing.



3.2 Random propagation of Information Shares

To expand routes, an ideal random propagation algorithm spreads information shares as dispersively as probable. Typically, this means propagating the share further than from its source.[8][9] At the same time, it is extremely necessary to have an energy resourceful propagation, which calls for limiting the number of randomly propagated hops. The experiment here lies in the random and distributed nature of the propagation: 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 the security's point of view. To tackle this issue,some control needs to be imposed on the random propagation process to ensure that in each step the share is more likely to be forwarded outwards from the source.[8][9] We develop four distributed random propagation mechanisms, which approach this goal in various degrees.

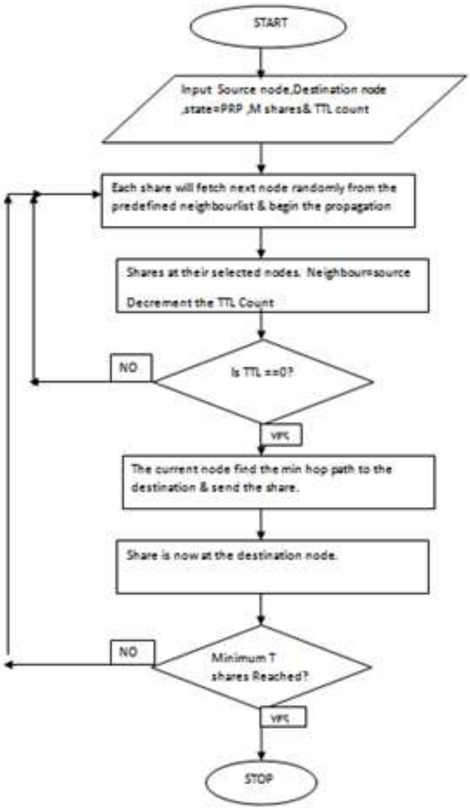
3.2.1) Purely Random Propagation (Baseline Scheme): **In PRP,**

Information shares are propagated based on one-hop neighborhood information. More exactly, a sensor node maintains a neighbor list, which holds the ids of all the nodes that are within its receiving range. When a source node wants to send information shares to the sink, it includes a TTL of initial value *N* in each share. Itrandomly picksa node from its neighbor list (this node cannot be the sourcenode) and relays the share to it, and so on. When the TTLreaches 0, the final node receiving this share stops the randompropagation of this share, and starts routing this share towardsthe sink using normal min-hop routing. The ANDERER scheme is a special case of PRP with $N = 1$.The main disadvantage of PRP is that its propagation efficiencycan be low, because a share may be propagated back and forthmultiple times between neighboring hops it increasing the value of TTLdoes not fully address this problem. This is because the randompropagation process reaches steady state under a large TTL,and its distribution will no longer change even if the TTLbecomes larger. .[8][9]

Algorithm for PRP

Input N=100,d=10km Shares=4,Source_node ,TTLdestination_node and datapacket;
Divide ***Data Packet*** into 4 equal shares (sub-packets)
Create 50 routing tables
Feed the neighbours information i.e. ***identifier of neighbouring node*** and
distance from source
Fetch data from routing table and send share1 to some neighbour within
transmission range
Fetch data from routing table and send share2 to some neighbour within
transmission range
Fetch data from routing table and send share3 to some neighbour within
transmission range
Fetch data from routing table and send share4 to some neighbour within
transmission range
NodeModule1 (source,destination,TTL,Share1);
NodeModule2(source, destination, TTL, Share2);

NodeModule3 (source, destination, TTL, Share3);
NodeModule4 (source, destination, TTL, Share4);



3.2.1) Non-repetitive Random Propagation:

NRRP is based onPRP, but it expands the propagation efficiency by recordingall the nodes that the propagation has pass through so far. Morespecifically, NRRP adds a "node-in-route" (NIR) field to theheader of each share. Initially, this field is empty. Starting fromthe source node, whenever a node propagates the share to thenext hop, the id of the up-stream node is joined to theshare's NIR field. Nodes included in NIR are excepted fromthe random pick of the next hop of propagation. This nonrepetitivepropagation assurances that the share will be relayedto a different node in each stage of random propagation, leadingto better propagation efficiency.

3.2.2) Directed Random Propagation: **DRP** Improves the propagationeffectiveness 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 tothe next node, the relaying node first substitutes the old content inthe LHNL field of the share by its neighbor list. When the nextnode receives the share, it compares the LHNL field againstits own neighbor list, and randomly picks one node from itsneighbors that are not in the LHNL. It then decrements theTTL value, updates the LHNL field, and relays the share to thenext hop, and so on. .[8][9] Every time the LHNL fully similarities with orcontains the relaying node's neighbor list, a random neighbor isdrawn, just as in the case of the PRP scheme. According to thispropagation method, DRP reduces the chance of propagatinga share back and forth by eliminating this type of propagationwithin any two immediate consecutive steps. Compared withPRP, DRP attempts to push a share outward away from the source, and thus leads to better propagation efficiency for agiven TTL value.

4) Multicast Tree-assisted Random Propagation:

TheMTRP scheme aims at actively improving the energy efficiencyof random propagation while preserving the dispersiveness ofDRP. Among the 3 different routes taken by the shares, theroute on the bottom right is the most energy efficient becauseit has the shortest end-to-end path. So, in order to improveenergy efficiency, the shares should be best propagated in thedirection of the sink. Conventionally, directional routing requires location informationof both the source and the destination nodes, andsometimes the intermediate nodes. .[8][9] Examples of this type oflocation-based routing are GPSR (Greedy Perimeter StatelessRouting) and LAR (Location-Aided Routing). Location informationmainly relies on GPS in each node, or on somedistributed localization algorithms. The high cost and the lowaccuracy of localization are the main drawbacks of these twomethods, respectively.MTRP involves directionality in its propagation processwithout needing location information. More specifically, afterthe deployment of the WSN, MTRP requires that the sinkconstructs a multicast tree from itself to every node in thenetwork. Such a tree-construction operation is not unusualin existing protocols, and is typically conducted via floodinga "hello" message from the sink to every node. Once thismulticast tree is constructed, a node knows its distance (innumber of hops) to the sink and the id of its parent node.We assume that each entry in the neighbor list maintained bya node has a field recording the number of hops to the sinkfrom the corresponding neighbor. Under MTRP, the header ofeach share contains two additional fields: max*hop*and

min*hop*.The values of these two parameters are set by the source tomax*hop*= *ns* + ®1 and min*hop*= *ns* ¡ ®2, where *ns* is thehop count from the source to the sink, and ®1 and ®2 are nonnegativeintegers ith®1 · ®2. The parameter ®1 controlsthe limit that a share can be propagated away from the sink,
The parameter®2 controls the propagation area toward the sink, i.e., the righthalf of the circle. A small ®2 makes the propagation of a sharebe dispersed away from the center line connecting the sourceand the link and forces them to take the side path, leading tobetter dispersion.Before a node begins to pick the next relaying node from itsneighbor list, it first filters out neighbors that are in the LHNL,just as in the case of DRP. Next, it filters out nodes that havea hop count to the sink greater than max*hop*or smaller thanmin*hop*. The next relaying node will be randomly drawn fromthe remaining neighbors. In case the set of remaining nodesafter the first step is empty, the second step will be directlyapplied to the entire set of neighbors.

EENDMRP

In wireless sensor networks routing is an essential technique for discovering multiple paths. The classical multipath routing are, Originally for load balancing; because traffics emanating from the source to destination are distributed over several pair of multiple node Disjoint paths. Secondly the delivery of reliable data is guaranteed through multipath routing. In multipath routing load balancing is precise essential because of it has the ability to distribute the utilization of energy over several nodes leading to prolong network lifetime. Whenever the Duplicating data delivery are sent through multiple paths, the tracing of observation applications is hugely enhanced and is more
specific at the expense of extra energy cost.

Energy-Efficient Multi-Path Routing

In the Energy-Efficient Multi-Path Routing in Wireless Sensor Networks which is a reactive routing protocol. In the network, each node may serve as a source and a sink node in the same time. The route discovery mechanism provides the multiple paths among source and
destination by using shared nodes in the search tree and query tree. The amount of control messages employed in the multiple route construction is consider high, because in order to construct query tree and search tree, query messages and search messages are to be broadcast in the network. These messages are sent from the source nodes and sink correspondingly. To achieve energy efficiency in routing protocols can be done usually through Groups jointly uniquely different from each other excluding the source node S and the sink node correspondingly. To choose the best path for path construction phase, the path cost function is used once the REEQ reach to sink node. The path cost computation is highlight through the following equation:[9]

Pc= E + H+D (1)

With H representing the number of hops to the sink node y when select next hop; E representing the minimum energy node in the path and D is signifying end-to-end delay. Therefore the path cost function takes the

minimum node energy in the path, the number of hop The selection benchmark used to
choose the best path in our proposed node disjoint multipath method is the path cost function, with the notion of employing in our proposed method. In definition the path Z is comprise of L nodes consists (L-1) of links, the path cost PZ denotes the calculation of specific link costs lu (u+1) along with the path. This is illustrated below as:[11]

$$P_Z = l_1 + l_2 + \dots + l_{L\ (l+1)} = \sum_{u=1}^{L-1} l_{u(u+1)}$$

Disjoint Multipath Routing: In sensor-disjoint path routing, the primary path is available whereas the alternate paths are less desirable as they have longer latency. The disjoint makes those alternate paths independent of the primary path. Thus, if a failure occurs on the primary path, it remains local and does not affect any of those alternate paths[12]

Conclusion

In this paper we identify two different basic types of data dissemination service for wireless embedded devices,” insider DoS attacks exploiting the epidemic propagation 26th IEEE Real-Time System Symposium, December strategies used by Deluge. They are Higher-version 2005. Advertisement attack, False Request attack, Larger- [6] L. A. Phillips, “Aqueduct: Robust and efficient code numbered Page attack, Lower-version Adv attack, and propagation in heterogeneous wireless sensor networks,” Same-version Adv attack. based on

DOI: 10.18535/Ijecs/v5i1.4

this protocol we can steer clear of this types of attacks in wsn in future

REFERENCES

1. ShazanaMdZin , Nor BadrulAnuar , Miss Laiha Mat Kiah , Ismail AhmedySurvey of secure multipath routing protocols for WSNs Journal of network and computer application 55(2015) 123 – 153
2. A Saranya Randomized Multipath Routes For Secure Data Delivery In Wireless Sensor Networks (IJLTET) 2011
3. C.Muthuramalingam, A.Karthikeyan, R.Bharathiraj, M.Muthukummaar, S.Edwin Randomized Routes For Secure Data Transmission Using Wireless Sensor Networks ISSN: 2250–3005 2010
4. Dr. A. SenthilkumarSecure Multipath routing Protocols in Wireless Sensor Network: a survey Analysis (IJCSITS), Vol. 3, No. 1, 2013
5. Muhammad juwaini, Raedalsaqour, Mahaabdelhaq, Ola alsukour a review on wep wireless security protocolissn: 1992-8645 vol. 40 no.1 2010
6. Abdulaleem Ali Almazroi, Ma Ngadi Energy Efficient Node Disjoint Multipath Routing To Improve Wireless Sensor Network Lifetime ISSN: 1992-8645 2011
7. Manivannan.P,Manivannan.DA Study on Secure Data Collection Mechanism for Wireless Sensor Networks (IJET) 2013
8. U.SenthilKumaran&IlangoParamasivamKey Pre-Distribution Scheme For Randomized Secured Routing In Wireless Sensor NetworksISSN: 1992-8645 2010
9. Shio Kumar Singh , M P Singh , and D K SinghRouting Protocols in Wireless Sensor Networks – A Survey 1 2 3 (IJCSES) Vol.1, No.2, November 2010
10. DelanAlsoufi , Khaled Elleithy , Tariq Abuzaghleh and Ahmad Nassar Security In Wireless Sensor Networks – Improving The Leap Protocol (IJCSES) Vol.3, No.3, June 2012
11. Sheela.D, Srividhya.V.R, AsmaBegam, Anjali and Chidanand G.M.Detecting Black Hole Attacks in Wireless Sensor Networks using Mobile Agent(ICAIES'2012) July 15-16, 2012
12. Samira Kalantary , Sara TaghipourA survey on architectures, protocols, applications, and management in wireless sensor networksJACST3 (1) (2014) 1-11
13. Suresh Gowda G J , Mr. MallikarjunaSwamy S Deepak B LEfficient Multicast Routing Algorithms for Scalable Wireless Network e-ISSN: 2250-3021, p-ISSN: 2278-8719 Vol. 3, Issue 7 (July. 2013)
14. B.KarpH. T.Kung.Greedyperimeterstatelessroutingfor wirelessnetworks”August2000pp6566.
15. Yu ZHANG[1 3], Xing She ZHOU[1], Yi Ming JI[2], Yee Wei LAW[3], Marimuthu PALANISWAMI[3]Five Basic Types of Insider DoS Attacks of Code Dissemination in Wireless Sensor NetworksI. J. Communications, Network and System Sciences, 2009, 1, 1-89