ISSN 2347-3983

International Journal of Emerging Trends in Engineering Research, Vol.3. No.10, Pages : 12-17 (2015)
Special Issue of ICACSSE 2015 - Held on October 30, 2015 in St. Ann's College of Engineering & Technology, Chirala, AP, India
http://www.warse.org/IJETER/static/pdf/Issue/icacsse2015sp03.pdf

A NOVEL APPROACH OF MULTIPATH ROUTING FOR SECURED DATA COLLECTION

Mr. A.Sai Mohith[1], Mr.Y.Chitti Babu[2]

[1]*II M.Tech. - II Sem., Dept. of CSE, St. Ann's College of Engineering. & Technology.Chirala,*
Andhra Pradesh - ,523 187 INDIA,
nagigundala@gmail.com

[2]*Associate Professor, Dept. of CSE, St. Ann's College of Engg.& Tech., Chirala, A. P, INDIA*
ycb@gmail.com

Abstract:

WSN (Wireless Sensor Network) has a wide range of uses. Thus, security issues turn out to be progressively essential. We explore the issue of minimizing the disappointment rate of bundle conveyance in the vicinity of the change assaults and the specific sending assaults in a static WSN with one base station without utilizing extravagant encryption/decoding calculations. We propose a novel heuristic way to deal with this issue. Our methodology is in view of randomized multipath steering. At the point when a sensor hub needs to send a bundle to the base station, it makes three duplicates and sends these three duplicates to the base station through three ways. Among the three ways, two of them are chosen indiscriminately in light of a spreading over tree with the base station as the root. The base station acknowledges a bundle just in the event that it gets no less than two indistinguishable duplicates. We have reenacted our methodology. The reenactment results demonstrate that our methodology accomplishes an extremely low disappointment rate of parcel conveyance in the vicinity of a moderately high rate of noxious sensor hubs.

INTRODUCTION

A WSN comprises of countless sensors hubs and one or more base stations. Every sensor hub sends its information detected from the physical environment to its assigned base station. Normally, sensor hubs are battery fueled. In request to spare vitality, the force of handset of every sensor hub is kept low, prompting a short transmission range. As a result, information gathering is performed in a multi-jump manner. Each bundle began from a sensor hub needs to conveyed to the objective base station through a steering way. Distinctive directing structures, for example, trees have been proposed [1].

WSN has an extensive variety of utilizations, including military field observation, social insurance, country security, mechanical control, and keen green air ship[2]. In this way, arrange security turns out to be progressively essential. Sensor hubs have restricted preparing force, little stockpiling what's more, constrained vitality. These requirements make traditional security calculations unacceptable for WSNs. Along these lines, new methods considering these impediments are required.

WSN security has pulled in broad examination [2]-[8] .Various assaults may bring about numerous security issues. Among them are the change assault and the specific sending assault. In the change assault, a malignant sensor hub may adjust a parcel it gets and sends the off base parcel to the base station by means of a directing way. In the particular sending assault, a vindictive sensor hub might decline to forward a parcel, bringing about a bundle misfortune.

In this paper, we research the issue of minimizing the disappointment rate of parcel conveyance in the vicinity of the adjustment assaults and the particular sending assaults in a static WSN with one base station without utilizing lavish encryption/decoding calculations. The disappointment rate is equivalent to the rate of the aggregate number of parcels rejected by the base station over the aggregate number of parcels produced by all the sensor hubs. We propose a novel heuristic way to deal with this issue. Our methodology is taking into account the three duplicate techniques. At the point when a sensor hub produces a bundle, it makes three duplicates which are sent to the base station by means of three ways. Among the three ways, two of them are chosen aimlessly in light of a spreading over tree with the base station as the root. The base station acknowledges a bundle just in the event that it gets no less than two indistinguishable duplicates. We have mimicked our methodology. The recreation results demonstrate that our methodology accomplishes a low disappointment rate of bundle conveyance in the vicinity of a generally high rate of malevolent sensor hub.

RELATED WORK

A. *Modification Attack*

Just a couple endeavors have been made to handle the adjustment assault as such [9]. Utilizes a catching method to distinguish vindictive parcel adjusting assaults in WSNs. By the catching method, an advisory group structure is developed for every sensor hub. The board of trustees' structure incorporates a few boards of trustees' sets, and every advisory group set is intended for a particular correspondence join. Because of the microwave nature of the remote channel, neighboring sensor hubs inside of a sender's radio reach can catch the parcel the sender is transmitting. In this way, every bundle can be inspected by the sensor hubs of the board set amid sending.

In the event that a bundle is altered by a pernicious hub, the advisory group set will distinguish the mistake. Be that as it may, the catching system expends a lot of vitality proposes a methodology for recognizing the malignant hubs that alter or drop bundles. [8]The proposed methodology scrambles every bundle and adds some additional bits to the parcel to shroud the wellspring of the bundle. It includes a bundle check, a little number of additional bits to every bundle such that the base station can recuperate the wellspring of the parcel and make sense of the dropping proportion connected with each sensor hub. The directing tree structure progressively changes in every round so that conduct of every sensor hub can be seen in an extensive mixed bag of situations. The heuristic positioning calculations can identify most of the bad nodes with small false positive. Also gives an excellent review of the previous approaches to the modification attack problem and the selective forwarding attack problem.

B. *Node-Disjoint Multipath Routing*

It is generally concurred that multipath steering is a proficient answer for the change and particular sending assaults [4]-[8] ,[11]. Multipath steering diminishes the shot of a bundle being adjusted or dropped by a noxious sensor hub by utilizing diverse ways [12]. A review of multipath steering conventions is introduced in. Multipath directing can be either hub disjoint, or connections disjoint, or in part disjoint [13]. Presents a multipath convention to expand the transmission discovering so as to unwavering quality a move down way adjacent to the administration way if there should arise an occurrence of transmission disappointments is an augmentation to by considering secure and solid information gathering.

It enhances the convention's security by applying the mystery sharing technique. Proposes a productive N-to-1 multipath directing convention in view of a base spreading over tree and a learning component.Proposes a vitality effective crash mindful multipath directing for WSN. It discovers two crash free ways to diminish the number of crashes among the sensor hubs in the system. Proposes a Low-Interference Energy-effective Multipath Directing convention (LIEMRO) for WSNs. This convention goes for discovering so as to enhance bundle conveyance proportion, lifetime, and dormancy numerous obstruction minimized hub disjoint ways between source hubs and sink hub. Plans to enhance the Direct Diffusion calculation keeping in mind the end goal to permit multipath directing in an interactive media remote sensor system which experiences impedances.

The base station chooses ways which have disjoint hub between them. Proposes a dispersed, adaptable and restricted multipath look convention to find numerous hub disjoint ways between the sink hub and source hub, and a heap adjusting calculation to disperse the activity over the different ways found.

The entire past multipath based steering methodologies utilization static directing ways, which make it simple for the aggressors to discover the objective sensor hubs for assaults proposes a few plans that create randomized multipath courses, and diagnostically examines the security and vitality execution of the proposed plans. Broad recreations are led to confirm the legitimacy of the proposed plan.

OUR APPROACH

The objective WSN is static, i.e., the area of every sensor is altered. There is one and only base station 1. Every sensor hub has an arrangement of neighboring sensor hubs with which it can convey specifically. Every correspondence connection is bidirectional. The entire system is associated, i.e., for every sensor hub, there is a directing way between this sensor hub and the base station. At the point when a sensor hub creates a bundle, this parcel needs to be sent to the base station. No information conglomeration is performed amid information gathering.

We explore the issue of minimizing the disappointment rate of bundle conveyance in the vicinity of the alteration assaults what's more, the specific sending assaults in a static WSN with one base station without utilizing extravagant encryption/unscrambling calculations. Our goal is two folds. Firstly, we go for minimizing the disappointment rate of bundle conveyance. Also, our proposed heuristic arrangement makes it troublesome for the aggressors to assault the bundles from an arrangement of target sensor hubs.

A. *Initialization Phase*

Amid the initialization stage, our methodology develops a briefest way traversing tree T established at the base station with the greatest lifetime as proposed in , then doles out an interesting ID to every sensor hub in a disseminated manner. The ID of each sensor vi, indicated by IDi, is characterized as takes after.

Let $v_{i1}.v_{i2}, \cdots, v_i k$ be all the children of the base station in *T* sorted in anti-clock-wise order in the polar coordinate system with the base station as the pole.

- Assign a unique ID to each sub tree rooted at a child of the base station in *T*. The ID of the sub tree rooted at $v_{ij}$is *j*.
- For each sub tree rooted at a child of the base station in *T*, assign a unique rank to each sensor node in the sub tree. The rank of a sensor node in a sub tree is its rank in the depth-first traversal order of the sub tree.
- For each sensor node v_s, its ID, denoted by *IDs*, isa tuple (x_s, v_s), where $x_s$is the ID of the sub tree containing $v_s$rooted at a child of the base station in*T*, and $v_s$is the rank of v_s.

1. **COMPUTE-SUBTREE-SIZE(*sub treeID*).**

   This message is created by the base station, and sent to each sensor node in *T*. The parameter *sub treeID*is the ID of the sub tree rooted at a child of the base station.

2. **SUBTREE-SIZE(*size*)**

   Size is the size of the sub tree of *T* rooted at a sensor node that sends this message. If a leaf node receives COMPUTE-SUBTREESIZE(*sub treeID*), it will send SUBTREE-SIZE(1) to its parent. If a non-leaf sensor node receives a $SUBTREE - SIZE$(*size*) from each child, it will calculate the size of the subtree of *T* rooted at itself, and send this message to its parent.

3. **COMPUTE-ID(*rank*).**

   This message is created by the base station and sent to each sensor node, where *rank* is the rank of the receiver of this message. When a sensor node $v_i$receives this message, $v_i$will send a COMPUTE-ID($rank_j$) message to each child v_j, where $rank_j$ is the rank of v_j. The ranks of the children of $v_i$are computed as follows. Let $v_j 1$,$v_j 2$, · · · , $v_j m$ be all the children of v_i. The rank of v_{i1} is equal to $rank_i$+ 1, where $rank_i$is the rank of v_i. The rank of $v_j s$ (s = 2, · · · ,m) is equal to $rank_{j\ s-1}$+$rank_{j\ s-1}$, where $rank_{j\ s-1}$ is the rank of $v_{j\ s-1}$, and $size_{j\ s-1}$ is the size of the subtree rooted at $v_{j\ s-1}$.

Algorithm 1 Initialisation phase

Let *L* be a list of all the children of the base station in *T* sorted in anti-clock-wise order in the polar coordinate system with the base station as the pole;

```
For the base station:
subtreeID= 1;
for each child $v_i$in L do
Send COMPUTE-SUBTREE-SIZE(subtreeID) to vi;
subtreeID=subtreeID+1;
end for
```

```
$i$ = 1;
while$i \leq |L|$ do
if SUBTREE-SIZE($sizei$) is received from a child $vi$ then
Send COMPUTE-ID(1) to $v_i$;
$i = i$ + 1;
end if
end while
```

For each sensor node v_i:

```
$v_i.size$ = 0;
Receive COMPUTE-SUBTREE-SIZE(subtreeID) from the parent;
$v_i.x = subtreeID$;
        if$v_i$is not a leaf node then
for each child $v_j$of $v_i$do
Send COMPUTE-SUBTREE-SIZE(subtreeID) to $v_j$;
end for
for each child $v_j$of $v_i$do
Receive SUBTREE-SIZE($v_j.size$) from $v_j$;
$v_i.size = v_i.size + v_j.size$;
end for
else
$v_i.size$ = 1;
Send SUBTREE-SIZE($v_i.size$) to the parent;
end if
Receive COMPUTE-ID($rank$);
$v_i.y = rank$;
$rank$= $rank$ + 1;
if$v_i$is not a leaf node then
for each child $v_j$of $v_i$do
Send COMPUTE-ID($rank$) to $v_j$;
$rank$= $rank + v_i.size$;
end for
        end if
```

B. Randomized Multipath Routing

In the wake of building the spreading over tree T and relegating a one of a kind ID to every sensor hub, every sensor hub can begin sending its bundles to the base station.

At the point when a sensor hub creates a parcel to be conveyed to the base station, it makes three duplicates of the bundle and sends the three duplicates along three ways to the base station. All together to make it troublesome for the malevolent hubs to assault the parcels from certain objective sensor hubs, our methodology builds two ways at irregular. In particular, when a sensor hub $v_i$makes a parcel, it produces two regular numbers X and Y between 1 what's more, the greatest ID of the sub trees established at the base station's youngsters by utilizing an irregular number generator. The principal duplicate is sent to the base station along the way from $v_i$to the base station in T. The two ways for the second duplicate and the third duplicate are chosen as takes after.

Algorithm 2 Randomized multipath routing phase

For the base station:

```
if a copy of a packet is received for the first time then
        set a timer for this copy;
if the timer expires then
        if at least two identical copies have been received then
        Accept any one of the identical copies;
else
        Reject the packet;
        end if
end if
end if
```

For each sensor node vi:

```
if$vi$ generates a packet then
        Create three copies, $copy$1, $copy$2 and $copy$3 of thepacket;
        Generate two natural numbers $X$ and $Y$ between 1 and
        the maximum ID of the subtrees rooted at the base
        station's children by using a random number
        generators;
        Generate a unique ID for the packet;
        $packetid$= the ID of the packet;
        $creator$= the ID of $vi$;
        $packetdata$= data of this packet;
        for$copyid$= 1, 2, 3 do
switch$copyid$do
case 1:
        $subtreestogo$= 0;
case 2:
        $subtreestogo$= $X$;
```

```
case 3:
        subtreestogo= $Y$ ;
        Find the receiver of this copy;
        Send PACKET-DELIVERY(creator, copyid,
        packetid, subtreestogo, packetdata) to the
        receiver;
end for
end if

if PACKET-DELIVERY(creator, copyid, packetid,
        subtreestogo, packetdata) is received then
switch copyid do

case 1:

Send PACKET-DELIVERY(creator,copyid,packetid, subtreestogo, packetdata) to the parent in T;

case 2, 3:

        Find the receiver as discussed before;

if the receiver is in a different subtree rooted at a child of the base station then subtreestogo = subtreestogo − 1;

end if

        Send PACKET-DELIVERY(creator, copyid,
        packetid, subtreestogo, packetdata) to the
        receiver;

end if
```

CONCLUSION

We have explored the issue of minimizing the disappointment rate of parcel conveyance in the vicinity of the alteration assaults and the particular sending assaults in a static WSN with one base station, and proposed a novel heuristic methodology. Not at all like the past static multipath directing based methodologies, has our methodology built two arbitrary ways, which makes it troublesome for the aggressors to assault the bundles from certain target sensor hubs. We have mimicked our methodology by creating 20 system occasions. The reenactment results show that our methodology accomplishes a low disappointment rate of bundle conveyance in the vicinity of a generally high rate of malignant sensor hubs.

As future work, we expect to enhance our methodology in three noteworthy viewpoints. Firstly, we will search for another randomized multipath steering calculation to boost the system lifetime. Besides, we will propose another calculation for recognizing vindictive sensor hubs and fuse the calculation into our approach. Ultimately, we will diagnostically examine the security furthermore, lifetime execution of our methodology.

REFERENCES

1) H. W. JingjingFei and Y. Wang, "K-dag based lifetime aware data collection in wireless sensor networks," *International Journal of Wirelessand Mobile Networks*, vol. 5, no. 5, 2013.
2) J. P. Walters, Z. Liang, W. Shi, and V. Chaudhary, "Wireless sensornetwork security: A survey," *Security in distributed, grid, mobile, andpervasive computing*, vol. 1, 2007.
3) V. Rathod and M. Mehta, "Security in wireless sensor network: asurvey," *GanpatUniv J EngTechnol*, vol. 1, no. 1, pp. 35–44, 2011.
4) J. Sen, "A survey on wireless sensor network security," *InternationalJournal of Communication Networks and Information Security (IJCNIS)*,vol. 1, no. 2, pp. 55–78, 2009.
5) S. K. Singh, M. Singh, and D. Singhtise, "A survey on networksecurity and attack defense mechanism for wireless sensor networks,"*International Journal of Computer Trends and Technology*, vol. 4, no. 2,pp. 1–9, 2011.
6) C. Karlof and D. Wagner, "Secure routing in wireless sensor networks:Attacks and countermeasures," *Ad hoc networks*, vol. 1, no. 2, pp. 293–315, 2003.
7) K. Vishnu and A. J. Paul, "Detection and removal of cooperative black/gray hole attack in mobile ad hoc networks," *International Journal of Computer Applications*, vol. 1, no. 22, pp. 38–42, 2010.
8) C. Wang, T. Feng, J. Kim, G. Wang, and W. Zhang, "Catching packet droppers and modifiers in wireless sensor networks," in *Sensor, Mesh and Ad Hoc Communications and Networks, 2009. SECON'09. 6th Annual IEEE Communications Society Conference on*, vol. 23, no. 5.IEEE, 2012, pp. 835–843.
9) K.-F. Ssu, C.-H. Chou, and L.-W. Cheng, "Using overhearing technique to detect malicious packet-modifying attacks in wireless sensor networks," *Computer Communications*, vol. 30, no. 11, pp. 2342–2352, 2007.

10) B. Bates, A. Keating, and R. Kinicki, "Energy analysis of four wireless sensor network mac protocols," in *Wireless and Pervasive Computing (ISWPC), 2011 6th International Symposium on.* IEEE, 2011, pp. 1–6.
11) S. Mohammadi and H. Jadidoleslamy, "A comparison of link layer attacks on wireless sensor networks," *International journal on applications of graph theory in wireless ad hoc networks and sensor networks (GRAPH-HOC)*, vol. 3, no. 1, pp. 35–65, 2011
12) M. Radi, B. Dezfouli, K. A. Bakar, and M. Lee, "Multipath routing in wireless sensor networks: Survey and research challenges," *Sensors,*vol. 12, no. 1, pp. 650–685, 2012.
13) D. Ganesan, R. Govindan, S. Shenker, and D. Estrin, "Highly-resilient, energy-efficient multipath routing in wireless sensor networks," *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 5, no. 4, pp. 11–25, 2001.

AUTHORS :

Mr. A.SaiMohith Studying II M.Tech (CSE) in St. Ann's College of Engineering & Technology, Chirala, He completed B.Tech.(CSE) in 2013 in St. Ann's Engineering College, Chirala.

Mr.Y.ChittiBabu is presently working as Associate Professor Department of Computer science &

Engineering in St. Ann's College of Engineering and Technology, Chirala.He is pursuing Ph.D. in Computer Networks and Security inAcharyaNagarjuna University. He guided many U.G. & P.G projects. He has more than 11Years of Teaching and. he published 5 International Journals and 25 research Oriented Papers in various areas.