International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT

ELSEVIER SSRN

2019IJIEMR.Personal use of this material is permitted. Permission from IJIEMR must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works. No Reprint should be done to this paper, all copy right is authenticated to Paper Authors

IJIEMR Transactions, online available on 11th Jul 2019. Link :http://www.ijiemr.org/downloads.php?vol=Volume-08&issue=ISSUE-07

Title: SECURE ROUTING ON TRUST SENSING BASED FOR WSN TO AVOID MISBEHAVIOR OF NODES

Volume 08, Issue 07, Pages: 104–112.

Paper Authors

SHAMSHEKHAR S PATIL, JEEVITHA H M

Dr. AIT, Bangalore, India

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

SECURE ROUTING ON TRUST SENSING BASED FOR WSN TO AVOID MISBEHAVIOR OF NODES

SHAMSHEKHAR S PATIL[1], JEEVITHA H M[2]

[1]Associate Professor, Department of Computer Science and Engineering, Dr. AIT, Bangalore.
[2]M.Tech Student,Department of Computer Science and Engineering, Dr. AIT, Bangalore.
[1] shamshekhar.patil@gmail.com, [2] jeevithahm15@gmail.com

Abstract— Current research domain in wireless sensor networks (WSNs), shows an outstanding capacity via recognize and manipulate the tangible world with almost every technologies. As we know that the wireless sensor networks (WSNs) aiming at critical effect of the typical network attacks are caused due to insufficient supply of energy (power) and the bad deployment environment while data transmission. In our paper we made an analyze to consider a lightweight features on secure routing on trust sensing based system (SRTSS) and capability to with stand many common attacks concurrently, the selection algorithm for secure routing is also optimized by using Quality of Service (QoS) metrics and trust degree under consideration simultaneously. Simulation outcomes and performance studies gives that secure routing on trust sensing based system can enhance the effectiveness and security of WSNs.

Keywords— Wireless sensor networks (WSNs), trust degree, energy, attack, route, sensor nodes, security, QoS metrics,trust management (TM).

I. INTRODUCTION

Now a days wireless sensor networks (WSN) are trending as a new emerging technology and have increased attention in wireless communications in few years ago. Advertises cloud computing, the fast growth of Internet of Things (IoT), Social Network and Smart City development [1]-[3]. WSN accompanying the feature of inexpensive, deploying very quickly and self-enterprise performs an essential aspect in promotes the smart city for benefits. The ubiquitary sensing nodes may gather both substantial information of metropolitan atmosphere and in the circumstances of smart urban environment it will manage the private and non-private centres [5], [6]. However, the multi-hop conquer is at risk of numerous varieties of assaults because open, allotted and vital function of WSN [7]-[10], that has an extreme effect on informationand safety. Currently, the existing secure routing set of rules are typically assisted from particular misbehaviour or greedy strategy assaults, they are in essentially depend on encryption set of rules and authentication device, that are not applicable for the multi-hop assigned and energy forced in wireless sensor network [11]-[13].The studies gives a certain trust management (TM) is an efficient manner to clarify the safety issues in wireless sensor network [14]-[17], anyhow the current routing convention depend on trust crucial to assure protection of multi-hop message transmission, and a logics perhaps outline given in below. Primary, while strategy depend on trust can knob implicit assaults in WSN, again precise a few recent hazard.Secondary, trust is automatically distinct against alternative regular routing indicators, like variety of hops, lag or other QoS demands.

However, the best reasonable models are not remembering the particular worth of trust rate inside the scheme of routing convention.

Tertiary, we have convinced drawback in the existing conquer protocol depend on trust, which include dependency on unique route system/scheme or platform. In different words, if any modified occurs in the network protocol results may be worthless in security mechanisms [18]-[21].

Our paper proposes a secure routing on trust sensing based system for WSN to clear up the overhead in the network and the security for multi-hop while data communication in this case. And the simulation outcomes display the secure routing on trust sensing based system not only enhance the facts in security to multi-hop transmission network, yet additionally decreases overhead in the routing WSN successfully. The major improvement of our paper is encapsulated in below:

1. Our paper analyses the conduct of sensing nodes, such as the motion and power utilization of sensing nodes. The trust rate of sensing hub is check out to give these aspects, after which they consider trust degree route is determined as well as calculate the trust version of network is set up to get the optimum path from start node to end node. On equal point, the trust rate and QoS metric is blended as the conquer metrics to offer revise routing discovery by means of the usage of the semiring concept.
2. The secure routing on trust sensing based system is arranged formulation and running system of secure routing on trust sensing based are again defined in our paper. Proposed routing discovery is enforced to the secure conquer system to accomplish the effective and trustworthy in sending information. Towards the identical period, the preservation manner of secure routing on trust sensing based system is also provided to in addition make certain the security of information transmission.

II. ANALYSIS OF ATTACKS

These phase analyses numerous ordinary network assaults in WSN and excerpt their aspects to give backing as security guarantee of WSN considering the fact that network assaults purpose at unique gadgets using extraordinary methods.

The typical assaults perhaps splitting within routing protocol assaults and consider version assaults in keeping with different assault spot. Multi-hop broadcast compose the harm of routing convention assaults to wireless sensor network also deliberate than the common wireless connection network. Usually, the routing protocol assaults possibly branched into smooth assaults and tough assaults consistent with the conduct of attackers. Smooth assaults mean that venomous or egoistically or misbehaviour nodes divert or smash the delivery facts via acting or dishonest fictional direction, consisting of: blackhole assault which provides bogus applicable pathway data inside the request the routing, grayhole assault which dumps a few statistics packets purposely, sinkhole assault which assembles regional assets, wormhole assault which constructs fake hyperlinks aside way of conspiracy, sniffing assault that snoop conquer facts with the aid of studying traffic in the network, along with sybil assault which duplicate many existence. Tough assaults imply which virulent nodes harm the data communication via wrecking the prevailing transmitting sources, which includes: DoS assault which fatigue the sources of assaulting items, tampering assault that alters chase information and replay assault which involves bandwidth sarcastically.

Despite of fact that the trust management (TM) machine may want to cope with maximum of network assaults and enhance the security of network with the aid of encryption and trust system, it possibly will become the recent goal of attackers. At current, the typical accept as true with version assaults encompass: on-off assault, contradictory

conduct assault, greedy assault, bad mouthing assault and collusion assault. In adding, the trust restraint algorithm which maintain encryption or trustworthy system extensively used in wireless communication network does not always appropriate being overall wireless networks, due to the fact the algorithm for trust management makes a speciality of the consider calculation system and neglect the trust derivation method. In case, in arrange to make sure the correctness of trust evaluation, trust data is regularly replaced at some stage in trust source, that induce a big quantity of overhead, such TM is crucial to cover the useful of resource-confined WSN precisely. Consequently, the lightweight features on secure routing system proposed in our paper may assemble trust degree via conduct also electricity, and integrate by QoS to layout conquer metrics in order this SRTSS for decrease price may face up to various types of typical assaults. In affixing, sybil assaults along with sniffing assaults are hard to discovered trust based system, but, venue confirmation and frequency hopping era can essentially oppose them, but this is not always the outlook of this paper.

III. RELATED WORK

Many research works have been introduced which are undertaken based on trust in different area of domains. Many researchers carried out to predict the calculation of trust using various techniques from many methodologies in different domains; we have analyzed some of those based on their criteria.

O. Ozel et al., [1] Wireless systems made out of remarkable nodes accept a notably extended lifespan and exist feasible. Specific features of this system are the truth a certain nodes can harvest strength in the course of the period where conversation occur. Similarly, communication action of nodes demand to accommodate those harvested strength appearance in paper, remember expansion of point-to-point information sending among an electricity harvesting sender which is having restrained battery capability, speaking in a wireless declining route. We keep in mind couple of goals: expand the throughput via a cut-off date, and diminish the communication of entirety time of the conversation session. We enhance those goals by using governing the life series of transmit powers concern to strength garage quantity and element restraints. We, firstly take a look at premier down approach. Directional Water-filling is introduced set of rules that presents an easy and succinct interpolation of the essential optimized situations. It shows the optimized of an adaptive directional water-filling algorithm for the throughput increase problem. We clear up the transmission of entirety time diminish issue by using appeal alikeness to appeal throughput expand counterpart.

G. Ottman et al., [3] paper offers an adaptive access to harvesting electrical strength against routinely inspired piezoelectric aspect. The DC to DC converter with an adaptive manage set of rules harvested strength by accomplished 4 instances the charge of direct charging outside a converter. Moreover, the ratio is call to hold to enhance at higher photoelectric ranges. The control algorithm may be implemented to different dc to dc converter topologies. Here cause the permit of progress in advance machine designs based upon the anticipated photoelectric load as to be powered.

Pirzada and McDonald et al., [4] paper we brought a concept of acceptance in trust-based for connection, which gives an effective amount of dependability and honesty relevant work applicable being an ad-hoc network.

Y. Gao et al., [6] as heterogeneous WSN power utilization is not uniform, and the energy usage charge is less. This paper calculates the power intake of a dissimilar clustering in sensor system, and proposed a brand new power efficient routing set of rules as clustering in similar networks. A proposed procedure chooses a cluster head hub in line with the strength of hubs at some point of the running of the network, on the way to reap excessive insurance.

Adel et al., [11] paper, proposed a trust model and a metrics primarily depends on concept of statistic and possibility to discover and prevent DoS assaults in MANETs. In the clustering architecture, the nodes watchdog the packet rates they get hold of from nearby hubs. During a node outstrip the frequency range for numerous instances, it turns into pseudo. In the proposed device, cluster head plays an examine within the network to examine approximately the conduct of these fishy nodes, and conclude in step with trust metrics, refuse or preserving them within the network. The gadget proposed straightforward to put in force also it does not need any extra assets as implementation.

J M. Chang et al., [12] this method, we have got proposed a new system Co-operative Bait detection scheme (referred to as the CBDS) for discovery of mischievous nodes in MANETs underneath grey/collaborative blackhole assaults. The deal with neighboring hub is using as bait target deal with bait mischievous nodes to transmit RREP reply information, and mischievous node is identifying the use of an opposite tracing approach. Each recognizes mischievous node is stored inside a list of blackhole so that each one alternative node which takes part in the routing message is notified to prevent communication with all nodes in that list.

IV. ROUTING ALGORITHM

There are many routing algorithms proposed by researches which effectively hepls to reduced the routing overhead of network. Now a days many works are being carried out to enhance the algorithm in order to evaluate trust degree.

Mainly in our paper we are using algorithm to detect the malevolent of nodes

Algorithm- Disclosure or discovery of Malevolent Nodes

Input: A route request (RREQ) packet to node

Output: Discovering the node position for all control packets to this node do

if the packet is neither from nor to this node itself then

if request is duplicate route request then

isDuplicate route request is equal to true

end if

In first step

if isduplicate route request= true AND reward timer is imminent then

messaging that “it is not a recent request” and jump over all the next steps

end if

else

Drop counter is then incremented by 1

end if

In second step timers are set

Sense timer=current time

Reward timer=current time

In the third step sense timer is made to begin

Sense timer=current time+ sense time

Drop counter is incremented by 1

To sending for this packet we have to calculate the time

if the sending time is greater than sense timer then

drop counter is incremented by 1

else

Reward timer is begin like that

Reward timer=current time + reward time(trust value)

drop counter is decremented by 1

end if

end if

if drop counter is successfully incremented then

“mark all nodes present as malevolent” and stop

end if

end for

The following are the steps which are used for discovery of malevolent nodes:

1. The sensing node continues a list of single hop that includes identification of whole nodes inside its communication area.

2. While a start node craves to convey control packets to end nodes, it contains a frequency range of packet with starting value N in every manipulated packet.

3. The RREQ packets are overwhelm in the list of single hop.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

4. Every neighbor will again transmit RREQ packet with the aid of choosing the nodes that has highest energy battery. The procedure is replicated till the link is entrenched until the vacation spot.

5. The trust value is calculated primarily based at the revel in in conversation or with its recognition primarily based, if the price of the node is underneath 0.5 then the node popularity is low, if the value is excessive then the node reputation is excessive.

6. If frequency range in the packet is zero again a method is accompanied via using selection of node that allows attaining the end speed.

V. PROPOSED METHODOLOGY

1. Topology Module- This phase carries description utilized in constructing topology. It contains wireless network for constructing topology along with cellular nodes, every node running along with many medium.
These phases as consecutive steps:

- Topology build up for wireless network: These encompass sustainable contexts, configuration of nodes, and formation of topology.
- Assembling frequency range and bandwidth: Each and every node in the network topology will be nominated with convinced bandwidth and topology.
- Neighbor's identification: Now scheme as to recognize the specific neighbor node in a Euclidean range view was handled.
- Specifying the data transmission through single and multi-hop: From which node the information has to be dispatched and which node should acquire the information may be designated. Additionally how a lot quantity of data needs to be sent at the side of the time of sending the facts may be nominated.
- Simulations for specifying begin time and quit time: In NS2 complete action catches the location inside fraction of seconds. The action may be examined via the NAM window by each time. Considering this simulations start time and stop time perhaps distinct.

2. Algorithm for deploying nodes- These algorithms are chargeable for randomly deploying the nodes in the specified place. Here nodes can role inside the shown location. The incoming set of rules contains wide variety of nodes and gap bounded by nodes. The outcomes includes in the mapping of node identification and node point.

3. Formation of Routing Tables- It is a set of rules, mainly used to shape tables to route for all nodes. The table of routing will include data around alternative nodes inside the network in phrases of node identification and the range of every node corresponding to alternative nodes within the network. The formation of the routing table algorithm is needed to design the tables for route in the nodes that consists of node identifications, interval and accessible symbol.

4. Energy Module- Energy ideal, as carry out in, is a node attribute. The power version shows the stage of power in a cellular host. The power version in a node has a preliminary fee that is the extent of strength the node has at the starting of the simulation. This is referred to as initial Energy. Additionally it has a given strength usage for every packet it transmits and gets. Those are known as txPower_ and rxPower_.

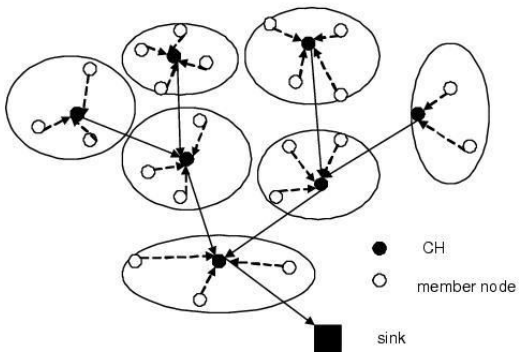


Figure: Cluster formation in WSN

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

5. Cluster Construction- The cluster-based architecture is used to assemble the topology. Each cluster node will select a cluster head (CH) based on high residual energy. To send packets, CH will choose source and destination node. If any malicious node is found on CH it will change the route and send packets. Then the nodes are removed from WSN. Again re-clustering formed and elected the next head.

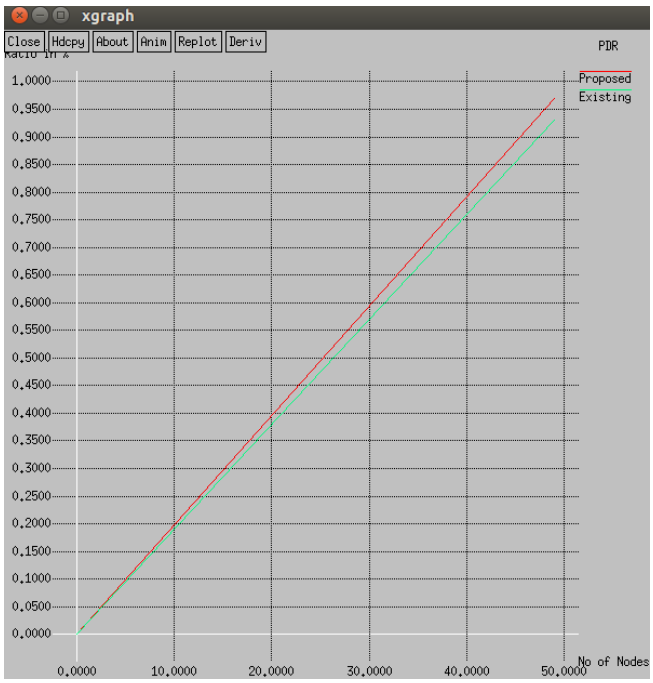
6. Attacker Module- In this implementation, the attacks may be categorized as manipulate and statistics attacks in network. We endorse a trusted routing protocol and simulate the nodes dropping the packets which decrease the achievement of the network. The mischievous node deliberately drops a packet which it has obtained and does no longer ahead to the following node; this creates a malicious hobby inside the network.

VI. PERFORMANCE EVALUATION

In our paper SRTSS the performance is analyzed by NS2. The misbehavior nodes may initiate grayhole assaults and bad mouthing attack in the simulation. The final step or outcome of the project undertaking is the final step wherein the system can be evaluated in phrases of overall performance and the consequences are proven the use of the graphs if the targets in the task which are described within the beginning are met or not. The performance is confirming the use of the values received. All of the experiment parameters evaluated the use of the graphs are shown in below.
From the below graphs **Red** line indicates the performance of proposed system of secure routing on trust sensing based system and **Green** line indicates the existing system of our paper. The X-axis consists of no. of nodes and Y-axis consisting according to their performances like overhead, throughput, delay, packet delivery ratio and energy efficiency respectively.

Graph 1.Throughput Performance

Throughput: Wide variety of packets sent and received in line with unit of time. It is expressed in terms of kilobytes per second (kbps). Average throughput of existing system value is 309.68 and proposed system value is 350.87.Throughput performances are illuminated in Graph 1.

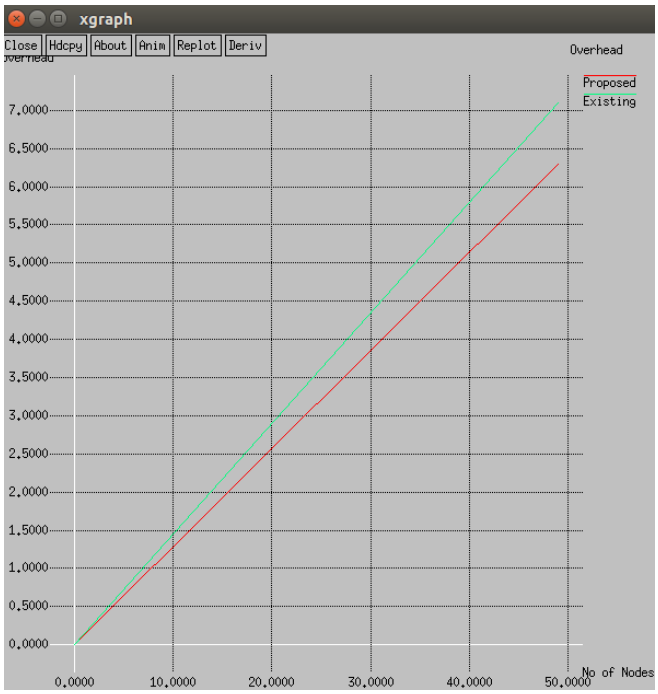


Graph 2.Packet Delivery Ratio

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

Graph 3.End to End Delay

Packet Delivery Ratio (PDR): The included rate of bundles translated by supply and the amount of bundles understand through target. PDR of existing system values of sent(s): 1102, received(r): 1029, ratio (r/s):0.9338, routing packet (f): 59 and loss(s-r): 73 and for proposed system values of sent(s): 1102, received(r): 1072, ratio (r/s):0.9728, routing packet (f): 66 and loss(s-r):60. PDR is expressed in terms of ratio (%). The packet delivery ratio in SRTSS is illuminated in Graph 2.



Graph 4.Overhead Performance

Graph 5.Energy Efficiency Performance

End to End Delay: Delay may be calculated by using dispatch time of packet by source – received time of packet by destination. It is expressed in milli seconds (ms). Average delay of existing system value is 624.873ms and proposed system value is 346.231ms. The end-to-end delay is illuminated in Graph 3.

Overhead: Overhead performance in wide range of routing packet handled. To enhance the influence we need to, transmit the information in numerous approaches against the opening node to the sink node. It is expressed in terms of load with respect to time. Overhead existing system value is 7.138 and proposed system value is 6.349. The overhead performance is illuminated in Graph 4.

Energy Efficiency: The energy usage and power efficiency of trust degree of sensor node organize are the remarkable troubles in internet of things set up. It may be used to enhance the power efficiency of the whole device. Perfect quantity of several nodes of the WSN topology is proposed for reinforcing energy effectiveness. It is expressed in terms of joules. The energy efficiency is illuminated in Graph 5.

VII. CONCLUSION AND FUTURE ENHANCEMENT

Our paper Secure Routing on Trust Sensing Based System (SRTSS) is to provide Quality of Service (QoS) metrics for wireless sensor networks (WSNs). It proposes a secure routing on trust sensing based system for WSN; it has capability to with stand many common attacks concurrently. In this case it will clear up overhead in the network and the multi-hop security for data communication. Analyses the conduct of sensor nodes, like motion and power consumption, consider trust degree calculation in network. Simulation outcomes displays that secure routing on trust sensing based system not only enhance the facts in security as multi-hop conversation network, also in addition to decrease the performance of overhead in the routing WSN efficaciously. Major drawback of this paper is inefficient energy, one layer security is not much secure and it works only for control messages.

In Future work, lightweight techniques for trust evaluation can be implemented to optimize the overhead of nodes.

REFERENCES

1. O. Ozel, K. Tutuncuoglu, J. Yang, S. Ulukus, and A. Yener, "Transmission with energy harvesting nodes in fading wireless channels: Optimal policies", IEEE J. Sel.Areas Commun., vol. 29, no. 8, pp.1732-1743, Sept. 2011.

2. N. Marlon, C. Jose, A. B. Campelo, O.Rafael, V.C.Juan, and J.S.Juan, "Active low intrusion hybrid monitor for wireless sensor networks", Sensors, vol. 15, no.3, pp.23927_23952,2015.

3. G. Ottman, A. Bhatt, H. Hofmann, and G. Leisure, "Adaptive piezoelectric energy harvesting circuit for wireless, remote power supply", IEEE Trans. Power Electron., vol. 17, no. 5, pp. 669_676, Sep. 2002.

4. A, Pirzada and C. McDonald, "Establishing Trust in Pure Adhoc Networks",in The 27th Australasian Conference on Computer Science, Dunedin, New Zealand, 2004.

5. W. K. K. Chin and K. L. A. Yau, "Trust and reputation scheme for clustering in cognitive radio networks". In Proc. Int. Conf. Frontiers Commun., Netw. Appl. (ICFCNA), Kuala Lumpur, Malaysia, Nov.2014, pp.1_6.

6. Y.Gao, H.W.Chris, J.J. Duan, and J.R. Chou, "A novel energy-aware distributed clustering algorithm for heterogeneous wireless sensor networks in the mobile environment", Sensors, vol. 15, no.10, pp.31108_31124, 2015.

7. J. -G. Choi and S. Bahk, "Cell-throughput analysis of the proportional fair scheduler in the single-cell environment", IEEE Trans. Veh. Technol., vol. 56, no, 2, pp.766_778, Mar. 2007.

8. K.B. Sourav and M. K. Pabitra, "SIR: A secure and intelligent routing protocol for vehicular adhoc network", IET Netw., vol. 4, no.6, pp.185_194, 2015.

9. E. Adel, K. Abdellatif, and E. Mohammed, "A new trust model to secure routing protocols against DoS attacks in MANETs", in Proc. 10th Int. Conf. Intell. Syst. Theories Appl. (SITA), Taipei, Taiwan, Oct. 2015, pp. 1_6.

10. J. –M. Chang. T.Po-Chun, W. G. Isaac, C. C. Han, and C. F.Lai, "Defending against collaborative attacks by malicious nodes in MANETs: A cooperative bait detection approach", IEEE Syst. J., vol. 9, no. 6, pp. 65_75, Jun. 2015.

11. P. G. Fernando, M. C. A. Rossana, T. O. Carina, and J. N. Souza, "EPMOst: An energy-efficient passive monitoring system for wireless sensor networks", Sensors, vol. 14, no. 3, pp. 10804_10828, 2015.

12. X. Du and H. H. Chen, "Security in wireless sensor networks", IEEE Wireless Commun., vol. 15, no. 4, pp.60_66, Aug. 2008.

13. J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on Internet of Things: Architecture, enabling technologies, security and privacy, and applications", IEEE Internet Things J., to be published.

14. Z. Liu, X. Yang, P. Zhao, and W. Yu, "An energy-balanced backpressure routing mechanism for stochastic energy harvesting wireless sensor networks", Int. J. Distrib. Sensor Netw. (IJDSN), vol. 12, no.8, pp.1_9, 2016.

15. H. Nakayama, S. Kurosawa, a. Jamalipour, Y. Nemoto, and N. Kato, "A dynamic anamoly detection scheme for AODV-based mobile ad hoc networks", IEEE Trans. Veh. Technol., vol. 58, no.5, pp. 2471_2481, Jun. 2009

16. Y. X. Liu, M. X. Dong, O. Kaoru, and A. F. Liu, "ActiveTrust: Secure and trustable routing in wireless sensor networks", IEEE Trans. Inf. Forensics Security, vol. 11, no. 2, pp. 2013_2027, Sep. 2016.

17. L. H. G. Ferraz, P. B. Velloso, and O. C. M. B. Duarte, "An accurate and precise malicious node exclusion mechanism for ad hoc networks", Ad Hoc Netw., vol. 19, no.6, pp.142_155, 2014.

18. S. Kurosawa, H. Nakayama, N. Kato, A. Jamalipour, and Y. Nemoto, "Detecting blackhole attack on AODV-based mobile adhoc network by dynamic learning method", Int. J. Netw. Secur., vol. 5, no. 9, pp. 14_21, 2007.

19. D. Zhu, X. Yang, W. Yu, and X. Fu, "Networking coding vs. Traditional routing in adversarial wireless networks", Int. J. ad Hoc Netw., vo. 20, no. 2, pp. 119_131, 2014.

20. P. Zhao, X. Yang, W. Yu and X. Fu, "A loose virtual clustering based routing for power heterogeneous MANETs", IEEE Trans. Veh. Technol., vol. 62, no. 5, pp. 2290_2302, Sep. 2013.

21. W. Yu and J. Lee, "Efficient energy sensitive routing protocols in mobile ad-hoc networks", in Proc. Process, Int. Conf. wireless Netw., Shanghai, China, Jun. 2002, pp. 3_9.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org