Impact Factor Value: 4.029 ISSN: 2349-7084
International Journal of Computer Engineering In Research Trends
Volume 4, Issue 10, October -2017, pp. 413-418 www.ijcert.org

Energy and Memory Clone Detection in Wireless Sensor Network

[1] Mr. Amatul Mateen Shamsiya, [2]Dr. G.S.S Rao
[1]Pursuing M.Tech(CSE), [2]Professor & HOD
[1,2]Nawab ShahAlam khan College of Engineering and Technology, Hyd
Email: amatulmateen.shamsiya@gmail.com ,profgssrao@gmail.com

Abstract: An associate degree energy-efficient location-aware clone detection protocol is planned in densely deployed WSNs, which may guarantee productive clone attack detection and maintain satisfactory network life. Specifically, the situation info of sensors is employed and every which way choose witnesses situated in an exceedingly ring space to verify the legitimacy of sensors and to report detected clone attacks. The ring structure facilitates energy-efficient information forwarding on the trail towards the witnesses and also the sink. Planned protocol are able to do one hundred clone detection likelihood with unsuspicious witnesses. Moreover, in most existing clone detection protocols with random witness choice theme, the desired buffer of sensors is typically keen about the node density, whereas, in the planned protocol, the desired buffer of sensors is freelance of hop length of the network radius. Planned protocol are able to do long network life by effectively distributing the traffic load across the network.

Keywords: wireless sensor networks, clone detection protocol, energy efficiency, and network lifetime

---

1. Introduction

Wireless sensors are widely deployed for a spread of applications, starting from environmental observance to telemedicine and objects chase, etc.. For efficient sensing element placement, sensors are sometimes not tamperproof devices and are deployed in places while not observance and protection, that makes them liable to completely different attacks. for instance, a malicious user could compromise some sensors and acquire their personal info. Then, it will duplicate the sensing elements and deploy clones in an exceedingly wireless sensor network (WSN) to launch a spread of attacks that is spoken because of the clone attack. because the duplicated sensors have constant info, e.g., code and scientific discipline info, captured from legitimate sensors, they'll simply participate in network operations and launch attacks. owing to the low value for sensing element duplication and preparation, clone attacks became one in all the foremost vital security problems in WSNs. Thus, it's essential to effectively discover clone attacks so as to confirm healthy operation of WSNs. to permit economical clone detection, usually, a collection of nodes arewaschosen, that is known as witnesses, to assist certify the legitimacy of the nodes within the network. The personal info of the supply node, i.e., identity and also the location info ar shared with witnesses at the stage of witness choice. once any of the nodes within the network desires to transmit information, it initial sends the request to the witnesses for legitimacy verification, and witnesses can report a detected attack if the node fails the certification. to attain productive clone detection, witness choice and legitimacy verification ought to fulfill 2 requirements: 1) witnesses ought to be every which way chosen, and 2) a minimum of one in all the witnesses will with

© 2017, IJCERT All Rights Reserved

success receive all the verification message(s) for clone detection. The primary demand is to form it tough for malicious users listen in the communication between this supply node and its witnesses in order that the malicious users cannot generate duplicate verification messages. The second demand is to form certain that a minimum of one in all the witnesses will check the identity of the sensing element nodes to work out whether or not there's a clone attack or not. to ensure a high clone detection likelihood, i.e., the likelihood that clone attacks are with success detected, it's vital and difficult to meet these necessities in clone detection protocol style. completely different from wireless terminal devices, wireless sensors are sometimes of smaller size and cheaper price, and have restricted battery and memory capability. Therefore, the planning criteria of clone detection protocols for sensing element networks shouldn't solely guarantee the high performance of clone detection likelihood however additionally contemplate the energy and memory potency of sensors. within the literature, some distributed clone detection protocols are planned, like irregular economical and Distributed protocol (RED) and line chooses Multi-cast protocol (LSM). However, most approaches in the main specialize in rising clone detection likelihood while not considering potency and balance of energy consumption in WSNs. With such reasonably approaches, some sensors could assign their batteries owing to the unbalanced energy consumption, and dead sensors could cause network partition, which can more have an effect on the conventional operation of WSNs. Christo Ananth et al. mentioned a system, during this proposal, a neural network approach is planned for energy conservation routing in an exceedingly wireless sensing element network. Our designed neural network system has been with success applied to our theme of energy conservation. The neural network is applied to predict most vital Node and choosing the cluster Head amongst the association of sensing element nodes within the network. once having a definite prediction regarding most vital Node, we'd wish to expand our approach in future to completely different WSN power management techniques and observe the results. during this proposal, we have a tendency to used discretional information for our experiment purpose; it's additionally expected to get a period information for the experiment in future and additionally by exploitation ad-hoc networks the energy state of the node is maximized. The choice of cluster Head is planned exploitation the neural network with feedforward learning methodology. and also the neural network found able to choose a node amongst competitive nodes as Cluster Head. Most existing approaches will improve the productive clone detection at the expense of energy consumption and memory storage, which cannot be appropriate for a few sensing element networks with restricted energy resource and memory storage.

2. Problem Statement

Different from wireless terminal devices, wireless sensors are sometimes of smaller size and cheaper price, and have restricted battery and memory capability. Therefore, the planning criteria of clone detection protocols for sensing element networks shouldn't solely guarantee the high performance of clone detection likelihood however additionally contemplate the energy and memory potency of sensors. To prolong the network life, i.e., the time period from the beginning of the network till the primary incidence of a sensing element that runs out of energy, it's vital to not solely minimize the energy consumption of every node however additionally balance the energy consumption among sensors distributive situated in numerous areas of WSNs.

3. Existing System

1.Some distributed clone detection protocols are planned, like irregular economical and Distributed protocol (RED) and Line-Select Multicast protocol (LSM).

2.In most existing clone detection protocols, the desired buffer size depends on the network node density, i.e., sensors want an oversized buffer to record the changed info among sensors in an exceedingly high-density WSN, and so the desired buffer size scales with the network node density.

3.Such demand makes the present protocols not thus appropriate for densely deployed WSNs. A wireless ad-hoc network, additionally referred to as IBSS freelance Basic Service Set, may be a electronic network during which the communication links are wireless. The network is ad-hoc as a result of every node is willing to

© 2017, IJCERT All Rights Reserved

forward information for different nodes, then the determination of that nodes forward information is created dynamically supported the network property. this can be in distinction to older network technologies during which some selected nodes, sometimes with custom hardware and diversely referred to as routers, switches, hubs, and firewalls, perform the task of forwarding the info. stripped-down configuration and fast preparation create unintended networks appropriate for emergency things like natural or human-induced disasters, military conflicts. a significant limitation with mobile nodes is that they need high quality, inflicting links to be oftentimes broken and re-established. Moreover, the information measure of a wireless channel is additionally restricted, and nodes operate restricted battery power, which is able to eventually be exhausted. Therefore, the planning of a mobile unintended network is very difficult, however this technology has high prospects to be able to manage communication protocols of the longer term. The cross-layer style deviates from the normal network style approach during which every layer of the stack would be created to work severally. The changed transmission power can facilitate that node to dynamically vary its propagation vary at the physical layer. this can be as a result of the propagation distance is usually directionally proportional to transmission power. This info is passed from the physical layer to the network layer in order that it will take optimum choices in routing protocols. a significant advantage of this protocol is that it permits access to info between the physical layer and high layers (MAC and network layer). However, these tools focus totally on the simulation of the whole protocol stack of the system. Though this will be vital within the proof-of-concept implementations of systems, the requirement for a lot of advanced simulation methodology is usually there. Agent-based modeling and simulation provide such a paradigm. To not be confused with multi-agent systems and intelligent agents, agent-based modeling originated from social sciences, wherever the goal was to gauge and think about largescale systems with various interacting "AGENT" or parts in an exceedingly wide selection of random things to watch international phenomena. in contrast to ancient AI systems with intelligent agents, agent-based modeling is analogous to the important world. Agent-based models are so effective in modeling bio-inspired and nature-inspired systems. In these systems, the fundamental interactions of the parts of the system, additionally known as a fancy adaptive system, are easy however lead to advanced international phenomena like emergence the trail Discovery method is initiated whenever a supply node must communicate with another node that it's no routing info in its table. each node maintains 2 separate counters: a node sequence range and a broadcast id. The supply node initiates path discovery by broadcasting a route request (RREQ) packet to its neighbors. once associate degree intermediate node receives a RREQ, if it's already received a RREQ with constant broadcast id and supply address, it drops the redundant RREQ and doesn't air it. If a node cannot satisfy the RREQ, it keeps track of the subsequent info so as to implement the reverse path setup.

3.1 Disadvantages

1.Most approaches in the main specialize in rising clone detection likelihood while not considering potency and balance of energy consumption in WSNs. 2.Some sensors could assign their batteries owing to the unbalanced energy consumption, and dead sensors could cause network partition, which can more have an effect on the conventional operation of WSNs. 3.Most existing approaches will improve the productive clone detection at the expense of energy consumption and memory storage, which cannot be appropriate for a few sensing element networks with restricted energy resource and memory storage.

4. Proposed System

1.Besides the clone detection likelihood, we have a tendency to additionally contemplate energy consumption and memory storage within the style of clone detection protocol, i.e., associate degree energy- and memory-efficient distributed clone detection protocol with random witness choice theme in WSNs.

2.Proposed protocol is applicable to general densely deployed multi-hop WSNs, wherever adversaries could compromise and clone sensing element nodes to launch attacks.

3.An energy-efficient ring based mostly clone detection (ERCD) protocol to attain high clone detection likelihood with random witness choice, whereas

© 2017, IJCERT All Rights Reserved

guaranteeing traditional network operations with satisfactory network life of WSNs.

4.1 Advantages

1.Energy efficient

2.Memory efficient

3.High network lifetime can be achieved

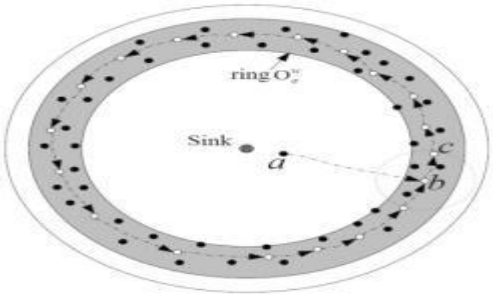
5. System Architecture

5.1 ERCD PROTOCOL

In this section, we have a tendency to introduce our distributed clone detection protocol, particularly ERCD protocol, which may succeed a high clone detection likelihood with very little negative impact on network life and restricted demand of buffer capability. The ERCD protocol consists of 2 stages: witness choice and legitimacy verification. In witness choice, a random mapping operates is used to assist every supply node every which way choose its witnesses. within the legitimacy verification, a verification request is distributed from the supply node to its witnesses, that contains the personal info of the supply node. If witnesses receive the verification messages, all the messages are going to be forwarded to the witness header for legitimacy verification, wherever witness headers are nodes liable for deciding whether or not the supply node is legitimacy or not, by comparison, the messages collected from all witnesses. If the received messages are completely different from existing record or the messages are terminated, the witness header can report a clone attack to the sink to trigger a revocation procedure. Initially, the network region is just about divided into h adjacent rings, wherever every ring includes a sufficiently sizable amount of sensing element nodes to forward on the ring and also the breadth of every ring is r. To modify the outline we have a tendency to use hop length to represent the stripped-down range of hops within the paper. Since we have a tendency to contemplate a densely deployed WSN, hop length of the network is that the quotient of the gap from the sink to the sensing element at the border of network region over the transmission vary of every sensing element, i.e., the gap of every hop refers to the transmission vary of sensing element nodes. TABLE I shows the mathematical symbols used during this section. The ERCD protocol starts with a breadth-first search by the sink node to initiate the ring index, and every one neighboring sensor sporadically exchange the relative location and ID info [23], [24]. After that, whenever a sensing element node establishes an information transmission to others, it's to run the ERCD protocol, i.e., witness choice and legitimacy verification, to verify its legitimacy.

In witness choice, a hoop index is every which way chosen by the mapping operate because the witness ring of node a. to assist relieve the traffic load in an exceedingly hot spot, the realm around the sink cannot be chosen by the mapping operation. After that, node a sends its personal info to the node situated in witness ring, then the node forwards the knowledge on the witness ring to make a hoop structure. within the legitimacy verification, a verification message from the supply node is forwarded to its witnesses. The ring index of node a denoted Oa, is compared with its witness ring index Oa w to work out consequent forwarding node. If Oa w > Oa, the message are going to be forwarded to any node situated in ring Oa + 1; otherwise, the message is going to be forwarded to any node in ring Oa one. This step will forward the message toward the witness ring of node a. The ERCD protocol repeats higher than operations till a node, denoted b, situated within the witness ring Oa w is reached. Node b stores the personal info of node a and forwards the message to any node situated in ring Oa w among its transmission vary denoted as c. Then, node c stores the knowledge and forwards the message to the node d, wherever the link (c,d) has the longest projection on the extension line of the directional link from b to c. The procedure is going to be recurrent till node b reappears within the transmission vary. Therefore, the witnesses of node a have a hoop structure, consisting of b, c, b as 1. Fig.1 Ring structure of witness

© 2017, IJCERT All Rights Reserved



1.

Fig.5.1.1 Ring structure of witness

In the legitimacy verification, node a sends a verification message as well as its personal info following theconstant path towards the witness ring as in witness choice. to boost the likelihood that witnesses will with success receive the verification message for clone detection, the message are going to be broadcast once it's terribly near the witness ring, particularly three-ring broadcasts, i.e., the message is going to be broadcast in Oa w one, Oa w and Oa w +1 as shown in figure 1,2.

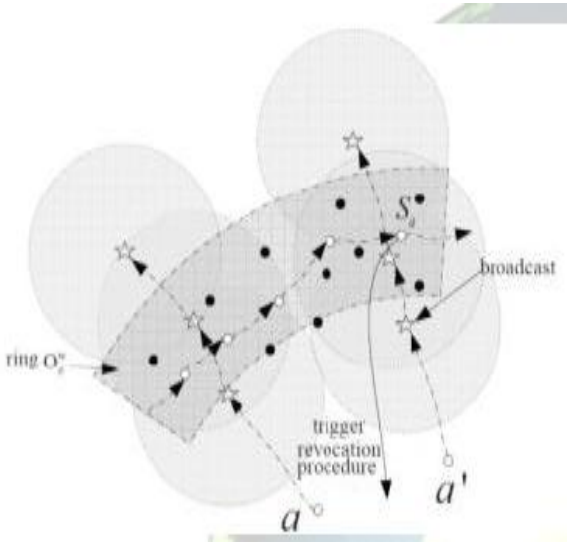


Fig.5.2.2 Legitimacy verification

In Theorem one, we have a tendency to prove that the three-ring broadcasts will make sure the network security, i.e., the clone detection likelihood is one, beneath the idea that each one witnessare unsuspicious. to work out whether or not there exists a lone attack or not, all the verification messages received by witnesses are forwarded to the witness header on theconstant route in witness choice. The sensing element nodes within the transmission route however not situated within the witness ring are known as the transmitters. The witness header of the supply node a, denoted by reserves, may be a sensing element situated in witness ring Oa w, meanwhile, it's additionally within the communication vary of the transmitter situated in ring index Oa w one or Oa w + one. The witness header Sais every which way was chosen by the transmitter within the neighboring witness ring, i.e., the ring of Oa w one or Oa w + one. If quite one copy or incorrect copies or terminated copies are received by the witness header, the ERCD protocol can trigger a revocation procedure; if no copy is received from the supply node owing to packet loss or silent cloned thenode, transmissions from the supply node won't be allowable.

6. Conclusion

In this paper, we've planned distributed energy economical clone detection protocol with random witness choice. Specifically, we've planned the ERCD protocol, which has the witness choice and legitimacy verification stages. Each of our theoretical analysis and simulation results hasincontestable that our protocol will discover the clone attack with nearly likelihood one since the witnesses of every sensing element node are distributed in an exceedingly ring structure that makes it simple be achieved by verification message. Additionally, our protocol is able to do higher network life and total energy consumption with an affordable storage capability of the info buffer. This can be as a result of we have a tendency to cash in of the situation info by distributing the traffic load everywhere WSNs, such the energy consumption and memory storage of the sensing element nodes around the sink node is mitigated and also the network life is extended. In our future work, we'll contemplate completely different quality patterns beneath varied network eventualities. sensing element networks are liable to node replication attacks. During this paper, we have a tendency to propose four distributed protocols for detecting these malicious attacks. The new protocols improve the state of the art by considerably reducing the number of memory area required, by equalization the memory and energy consumption across the network, and by raising the detection likelihood to almost 100also have some of thelimitations. they can't discover the replication attacks in an exceedingly mobile sensing element atmosphere.

© 2017, IJCERT All Rights Reserved

They believe the comparatively pricey public key cryptography. Our future work is to style replication detection protocols that use the key key cryptography and work for each static and mobile sensors.

References

[1] Z. Zheng, A. Liu, L. X. Cai, Z. Chen, and X. Shen, "ERCD: An energy-efficient clone detection protocol in wasns," in Proc. IEEE INFOCOM, Turin, IT, Apr. 14-19 2015, pp. 2436–2444.

[2] R. Lu, X. Li, X. Liang, X. Shen, and X. Lin, "GRS: The green, reliability, and security of emerging machine to machine communications," IEEE Communications Magazine, vol. 49, no. 4, pp. 28–35, Apr. 2013.

[3] Christo Ananth, A.NasrinBanu, M.Manju, S.Nilofer, S.Mageshwari, A.PeratchiSelvi, "Efficient Energy Management Routing in WSN", International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE), Volume 1, Issue 1, August 2012,pp:16-19

[4] Liu, J. Ren, X. Li, Z. Chen, and X. Shen, "Design principles and improvement of cost function based energy aware routing algorithms for wireless sensor networks," Computer Networks, vol. 56, no. 7, pp. 1951–1967, May. 2011.

[5] T. Shu, M. Krunz, and S. Liu, "Secure data collection in wireless sen-sor networks using randomized dispersive routes," IEEE Transactions on Mobile Computing, vol. 9, no. 7, pp. 941–954, Jul. 2010.

[6] Uma Vasala and Dr. G. R. Sakthidharan," Effective Key Management In Dynamic Wireless Sensor Networks"..”International Journal of Computer Engineering in Research Trends., vol.4, no.7, pp. 308-312, 2017.

[7] K.MANIMALA and .RANJITH," Mobile Transmission Using Rigorous Data for Wireless Sensor Networks"..”International Journal of Computer Engineering in Research Trends., vol.1, no.6, pp. 436-446, 2014.

[8] P. G. V. SURESH KUMAR1 , SEELAM SOWJANYA," Developing An Enterprise Environment by Using Wireless Sensor Network System Architecture"..”International Journal of Computer Engineering in Research Trends., vol.2, no.10, pp. 902-908, 2015.

[9] JALAGAM NAGAMANI, K.SUMALATHA," EAACK: Secure IDS for Wireless Sensor Networks"..”International Journal of Computer Engineering in Research Trends., vol.1, no.6, pp. 461-469, 2014.

[10] G V N LAKSHMI PRIYANKA, TELUGU KAVITHA, B SWATHI and P.SUMAN PRAKASH," Significance of DSSD towards Cut Detection in Wireless Sensor Network"..”International Journal of Computer Engineering in Research Trends., vol.2, no.1, pp. 8-12, 2015.

[11] Kumara Swamy,E Ramya," A Contemplate on Vampire Attacks in Wireless Ad-Hoc Sensor Networks"..”International Journal of Computer Engineering in Research Trends., vol.2, no.12, pp. 834-836, 2015.

[12] Shital Patil , Vishaka Patil , Rupali Warke , Priyanka Patil," Prevention of Packet Hiding Methods In Selective Jamming Attack"..”International Journal of Computer Engineering in Research Trends., vol.3, no.4, pp. 194-196, 2016.

© 2017, IJCERT All Rights Reserved