Clone Detection In Wsn's For Optimization Of Energy And Memory Efficiency

GUTTA VENKATESH* **MAHESH AKUTHOTA****

PG SCHOLAR*, ASSISTANT PROFESSOR**

Department Of Cse, Visvesvaraya College Of Engineering And Technology, M.P Patelguda,
Ibrahimpatnam (M), Ranga Reddy (D), And India

ABSTRACT

The Energy-Efficient location-aware clone detection protocol in densely deployed WSNs, which can guarantee successful clone attack detection and maintain satisfactory network lifetime. Specifically, we exploit the location information of sensors and randomly select witnesses located in a ring area to verify the legitimacy of sensors and to report detected clone attacks. The ring structure facilitates energy-efficient data forwarding along the path towards the witnesses and the sink. We theoretically prove that the proposed protocol can achieve 100 percent clone detection probability with trustful witnesses. We further extend the work by studying the clone detection performance with un trustful witnesses and show that the clone detection. Probability still approaches98 percent when 10 percent of witnesses are compromised.

I INTRODUCTION

Moreover, in most existing clone detection protocols with random witnessselection scheme, the required buffer storage of sensors is usually dependent on the node density, protocol, the required bufferstorage of sensors is independent of n but a function of the hop length of the network radius h, i.e.,.Extensive simulations demonstrate that our proposed protocol can achieve long network lifetime by effectively distributing the trafficload across the network.Wireless sensors have been widely deployed for a varietyof applications, ranging from environment

Monitoring to tele medicine and objects tracking, etc. [2]–[4]. For costeffective sensor placement, sensors are usually not tamper proofdevices and are deployed in places without monitoring and protection, which makes them prone to different attacks. For example, a malicious user may compromise some sensors and acquire their privateinformation. Then, it can duplicate the sensors and deployclones in a wireless sensor network (WSN) to launch avariety of attacks [10],which is referred to as the cloneattack [11]–[13]. As the duplicated sensors have the sameinformation, e.g., code and cryptographic information,captured from legitimate sensors, they can easilyparticipate in network operations and launch attacks.Due to the low cost for sensor duplication anddeployment, clone attacks have become one of the mostcritical security issues in WSNs. Thus, it is essential toeffectively detect clone attacks in order to ensure healthyoperation of WSNs.To allow efficient clone detection, usually, a set of nodesare selected, which are called witnesses, to help certify thelegitimacy of the nodes in the network. The privateinformation of the source node, i.e., identity and thelocation information are shared with witnesses at the stageof witness selection. When any of the nodes in the networkwants to transmit data, it first sends the request to thewitnesses for legitimacy verification, and witnesses willreport a detected attack if the node fails the certification.To achieve successful clone detection, witness selectionand legitimacy verification .

II RELATED WORK

As one of the utmost important security issues, clone attackhas attracted people's attention. There are many works [14],[15],[16] that studies clone detection protocols in the literature,which can be classified into two different categories,i.e., centralized and distributed clone detection protocols. Incentralized protocols, the sink or witnesses generally locatein the center of each region, and store the private informationof sensors. When the sink or witnesses receive the privateinformation of the source node, they can determine whetherthere is a clone attack by comparing the private informationwith its pre-stored records normally, centralizedclone detection protocols have low overhead and runningcomplexity. However, the security of sensors' private informationmay not be guaranteed, because the malicious userscan eavesdrop the transmission between the sink node andsensors. Moreover, the network lifetime may be dramaticallydecreased since the sensor nodes close to the sink willdeplete their energy sooner than other nodes.Different from centralized protocols, in distributed clonedetection protocols, a set of witnesses are selected to matchwith every sensor [10], [11], which prevents the transmissionbetween the sink and sensors from being eavesdroppedby malicious users. There are three different types of witnessselection schemes in distributed clone detection protocols:i) deterministic selection, ii) random selection, andiii) semi-random selection. The deterministic witness selectionbased clone detection protocols like RED [10] choosethe same set of witnesses for all sensor nodes. By usingdeterministic witness selection, a low communication overheadand a high clone detection probability can be achieved.

III Energy and Memory Efficient Clone Detection inWireless Sensor Networks

In the literature, some distributed clone detectionprotocols have been proposed, such as RandomizedEfficient and Distributed protocol (RED) [10] and Line-Select Multi-cast protocol (LSM) [11]. However, mostapproaches mainly focus on improving clone detectionprobability without considering efficiency and balance ofenergy consumption in WSNs. With such kind ofapproaches, some sensors may use up their batteries due tothe unbalanced energy consumption, and dead sensors maycause network partition, which may further affect thenormal operation of WSNs. Christo Ananth et al. [3]discussed about a system, In this proposal, a neuralnetwork approach is proposed for energy conservationrouting in a wireless sensor network. Our designed neuralnetwork system has been successfully applied to ourscheme of energy conservation. Neural network is appliedto predict Most Significant Node and selecting the GroupHead amongst the association of sensor nodes in thenetwork. After having a precise prediction about MostSignificant Node, we would like to expand our approachin future to different WSN power management techniquesand observe the results. In this proposal, we used arbitrarydata for our experiment purpose; it is also expected togenerate a real time data for the experiment in future andalso by using adhoc networks the energy level of the nodecan be maximized.

IV ERCD PROTOCOL

In this section, we introduce our distributed clonedetection protocol, namely ERCD protocol, which canachieve a high clone detection probability with littlenegative impact on network lifetime and limitedrequirement of buffer storage capacity. The ERCDprotocol consists of two stages: witness selection andlegitimacy verification. In witness selection, a randommapping function is employed to help each source noderandomly select its witnesses. In the legitimacyverification, a verification request is sent from the sourcenode to its witnesses, which contains the privateinformation of the source node. If witnesses receive theverification messages, all the messages will be forwardedto the witness header for legitimacy verification, wherewitness headers are nodes responsible for determiningwhether the source node is legitimacy or not by comparingthe messages collected from all witnesses. If the receivedmessages are different from existing record or themessages are expired, the witness header will report aclone attack to the sink to trigger a revocation procedure.Initially, the network region is virtually dividedinto h adjacent rings, where each ring has a sufficientlylarge number of sensor nodes to forward along the ringand the width of each ring is r. To simplify the descriptionwe use hop length to represent the minimal number ofhops in the paper. Since we consider a densely deployedWSN, hop length of the network is the quotient of thedistance from the sink to the sensor at the border ofnetwork region over the transmission range of each sensor,i.e., the distance of each hop refers to the transmissionrange of sensor nodes.

The ERCD protocol starts with a breadth-firstsearch by the sink node to initiate the ring index, and allneighbouring sensors periodically exchange the relativelocation and ID information. After that,whenever a sensor node establishes a data transmission toothers, it has to run the ERCD protocol, i.e., witnessselection and legitimacy verification, to verify itslegitimacy. In witness selection, a ring index is randomlyselected by the mapping function as the witness ring ofnode a. To help relieve the traffic load in hot spot, the areaaround the sink cannot be selected by the mappingfunction. After that, node a sends its private information tothe node located in witness ring, and then the nodeforward the information along the witness ring to form aring structure. In the legitimacy verification, a verificationmessage of the source node is forwarded to its witnesses.The ring index of node a, denoted Oa, is compared with itswitness ring index Oa W to determine the next forwardingnode. If Oaw > Oa, the message will be forwarded to any node located in ring Oa + 1; otherwise, the message will beforwarded to any node in ring Oa 1. This step can forwardthe message toward the witness ring of node a. The ERCDprotocol repeats above operations until a node, denoted b,located in the witness ring Oaw is reached. Node b storesthe private information of node a and forwards themessage to any node located in ring Oaw within itstransmission range, denoted as c. Then, node c stores theinformation and forwards the message to the node d,where link (c,d) has longest projection on the extensionline of the directional link from b to c. The procedure willbe repeated until node b reappears in the transmissionrange. Therefore, the witnesses of node a have a ringstructure

In the legitimacy verification, node a sends a verificationmessage including its private information following thesame path towards the witness ring as in witness selection.To enhance the probability that witnesses can successfullyreceive the verification message for clone detection, themessage will be broadcast when it is very close to thewitness ring, namely three-ring broadcasts, i.e., themessage will be broadcast in Oa

V PERFORMANCE ANALYSIS

In this section, the performance of the ERCDprotocol is evaluated in terms of clone detectionprobability, power consumption, network lifetime, anddata buffer capacity. At first, we prove that the clonedetection probability of the ERCD protocol can almostsurely achieve probability 1 under the scenario thatwitnesses are trustful in Subsection V-A. Then, we derivethe expression of energy consumption and networklifetime by using ERCD protocol, and obtain the ratio ofnetwork lifetime by using ERCD protocol over RED orLSM protocol in Subsection V-B. Finally, the requireddata buffer of the ERCD protocol is derived in SubsectionV-C.

Probability of Clone Detection

In distributed clone detection protocol withrandom witness selection, the clone detection probabilitygenerally refers to whether witnesses can successfullyreceive the verification message from the source node ornot. Thus, the clone detection probability of ERCDprotocol is the probability that the verification messagecan be successfully transmitted from the source node to itswitnesses. In ERCD protocol, the verification message isbroadcast when it is near the witness ring, i.e., in the ringssecurity. With such kind of method and assumption oftrustful witnesses, we can prove that at least one of thewitnesses can receive the message, i.e., the clone attackcan be detected with probability one. To simplify theanalysis, the transmission ranges of all sensor nodes, r, arethe same.

VI CONCLUSION

In this paper, we have proposed distributedenergy efficient clone detection protocol with randomwitness selection. Specifically, we have proposed theERCD protocol, which includes the witness selection andlegitimacy verification stages. Both of our theoreticalanalysis and simulation results have demonstrated that ourprotocol can detect the clone attack with almostprobability 1, since the witnesses of each sensor node isdistributed in a ring structure which makes it easy beachieved by verification message. In addition, our protocolcan achieve better network lifetime and total energyconsumption with reasonable storage capacity of databuffer. This is because we take advantage of the locationinformation by distributing the traffic load all over WSNs,such that the energy consumption and memory storage ofthe sensor nodes around the sink node can be relieved andthe network lifetime can be extended. In our future work,we will consider different mobility patterns under variousnetwork scenarios.

REFERENCES

[1] Z. Zheng, A. Liu, L. X. Cai, Z. Chen, and X. Shen,“ERCD: An energy-efficient clone detection protocolin wsns,” in Proc. IEEE INFOCOM, Turin, IT, Apr.14-19 2013, pp. 2436–2444.

[2] R. Lu, X. Li, X. Liang, X. Shen, and X. Lin, “GRS:The green, reliability, and security of emergingmachine to machine communications,” IEEECommunications Magazine, vol. 49, no. 4, pp. 28–35,Apr. 2011.

[3] Christo Ananth, A.Nasrin Banu, M.Manju, S.Nilofer,S.Mageshwari, A.Peratchi Selvi, “Efficient EnergyManagement Routing in WSN”, International Journalof Advanced Research in Management, Architecture,Technology and Engineering (IJARMATE), Volume 1,Issue 1, August 2015,pp:16-19

[4] Liu, J. Ren, X. Li, Z. Chen, and X. Shen, “Designprinciples and improvement of cost function basedenergy aware routing algorithms for wireless sensornetworks,” Computer Networks, vol. 56, no. 7, pp.1951–1967, May. 2012.

[5] T. Shu, M. Krunz, and S. Liu, "Secure data collectionin wireless sen-sor networks using randomizeddispersive routes," IEEE Transactions on MobileComputing, vol. 9, no. 7, pp. 941–954, Jul. 2010.

[6] P. Papadimitratos, J. Luo, and J. P. Hubaux, "Arandomized coun-termeasure against parasiticadversaries in wireless sensor networks,"

[7] IEEE Journal on Selected Areas in Communications,vol. 28, no. 7, pp. 1036–1045, Sep. 2010.

[8] R. Lu, X. Lin, T. H. Luan, X. Liang, and X. Shen,"Pseudonym changing at social spots: An effectivestrategy for location privacy in VANETs," IEEETransactions on Vehicular Technology, vol. 61, no. 1,pp. 86–96, Jan. 2012.

[9] Z. M. Fadlullah, M. Fouda, N. Kato, X. Shen, and Y.Nozaki, "An early warning system against maliciousactivities for smart grid communications," IEEENetwork, vol. 25, no. 5, pp. 50–55, May. 2011.

[10] R. Lu, X. Lin, X. Liang, and X. Shen, "A dynamicprivacy-preserving key management scheme forlocation based services in VANETs," IEEETransactions on Intelligent Transportation Systems,vol. 13, no. 1, pp. 127–139, Jan. 2012.

[11] M. Conti, R. D. Pietro, L. Mancini, and A. Mei,"Distributed detection of clone attacks in wirelesssensor networks," IEEE Transactions on Dependableand Secure Computing, vol. 8, no. 5, pp. 685–698,Sep.-Oct. 2011.

[12] Parno, A. Perrig, and V. Gligor, "Distributed detectionof node replication attacks in sensor networks," inProc. IEEE Symposium on Security and Privacy,Oakland, CA, USA, May. 8-11 2005, pp. 49–63.

[13] Y. Zeng, J. Cao, S. Zhang, S. Guo, and L. Xie,"Random-walk based approach to detect clone attacksin wireless sensor networks," IEEE Journal on SelectedAreas in Communications, vol. 28, no. 28, pp. 677–691, Jun. 2010.

[14] Zhu, S. Setia, S. Jajodia, S. Roy, and L. Wang,"Localized multicast: Efficient and distributed replicadetection in large-scale sensor networks," IEEETransactions on Mobile Computing, vol. 9, no. 7, pp.913–926, Jul. 2010.

[15] Y. Xuan, Y. Shen, N. P. Nguyen, and M. T. Thai, "Atrigger identification service for defending reactivejammers in WSN," IEEE Transactions on MobileComputing, vol. 11, no. 5, pp. 793–806, May. 2012.

[16] R. Lu, X. Lin, H. Zhu, X. Liang, and X. Shen.,"BECAN: A bandwidth-efficient cooperativeauthentication scheme for filtering injected false datain wireless sensor

networks," IEEE Transactions onParallel and Distributed Systems, vol. 23, no. 1, pp.32–43, Jan. 2012.

[17] J. Li, J. Chen, and T. H. Lai, "Energy-efficientintrusion detection with a barrier of probabilisticsensors," in Proc. IEEE INFOCOM, Orlando, FL,USA, Mar. 25-30 2012, pp. 118–126