ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 10, October 2018

A Novel Protocol for Energy and Memory Clone Detection in Wireless Sensor Network

V.Vinod Kumar [1], Dr.M.Sampath Kumar [2]

P.G. Scholar, Department of CS & SE, College of Engineering (A), Andhra University, Visakhapatnam, India[1]

Professor Department of CS & SE, College of Engineering (A), Andhra University, Visakhapatnam, India[2]

ABSTRACT: A power efficient location conscious clone detection protocol in densely deployed in WSNs that could assure hit clone assault detection and preserve exceptional network lifetime. Mainly the information of sensors is used and randomly selected to witness the hoop region to confirm the legitimacy of sensors and to record detected clone attacks. The ring structure facilitates power efficient statistics forwarding alongside the direction closer to witnesses and the sink. In this paper we propose an energy efficient clone detection protocol in densely deployed WSNs, which can guarantee successful clone attack detection and maintain satisfactory network lifetime. Specifically we exploit location information of sensors and randomly select witnesses located in ring area to verify legitimacy of sensors and to report detected clone attacks. The ring structure facilitates energy efficient data forwarding energy along the path towards the witnesses and sink. We theoretically prove that the proposed protocol can achieve 100 percent clone detection probability with trustful witnesses. As the duplicated sensors have identical statistics. Due to the low cost for sensor duplication and deployment, current clone detection protocols with random witness choice scheme, the desired buffer storage of sensor is commonly depending on the node frequency, even in our proposed protocol, the desired buffer storage of sensors of objective n but a characteristic of n of the hop duration of the network radius.

KEYWORDS: Wireless sensor networks, clone detection, memory

I. INTRODUCTION

Wireless sensor networks have seen tremendous advances and utilization in the past two decades .starting from petroleum exploration, mining, weather and even battle operations all of these require sensor applications. One reason behind the growing popularity of sensor is that they can work in remote areas without manual intervention. All the user needs to do is to gather the data sent by the sensors, and with certain analysis extract meaningful information from them. Usually sensor applications involve many sensor deployed together. These sensors form a network and collaborate with each other to gather data and send it to the base station. The base station acts as the control centre where the data from the sensors are gathered for further analysis and processing. In a nutshell, a wireless sensor network (WSN) is a wireless network consisting of spatially distributed nodes which use sensors to monitor physical or environmental conditions. These nodes combine with routers and gateways to create a WSN system.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 10, October 2018

The basic components of a node are

Sensor and actuator – an interface to the physical world designed to sense the environmental parameters like pressure and temperature.

1. Controller – is to control different modes of operation for processing of data.
2. Memory – storage for programming data.
3. Communication- a device like antenna for sending and receiving data over a wireless channel.
4. Power supply - supply of energy for smooth operation of a node like battery.

II. RELATED WORK

In literature survey, providing the related background and work on each part is listed as:

Z.Zheng[1] proposed an energy-efficient location-aware clone detection protocol in densely deployed WSNs, which can guarantee successful clone attack detection and maintain satisfactory network lifetime. An area based scheme is proposed by Naruephiphat. In this scheme, a node having maximum number of neighbours is selected as the central node. Then, the network is divided into sub-areas. Each sub-area has equal angle around the central node. A witness node is selected in each sub-area using the method similar to the one used to select the central node. A node sends its location-claim to the witness node of its area. If a witness node detects a location conflict, then it broadcast a conflict notification to all nodes in the network. On reception of claims without conflict, the witness node sends these claims to the central node for further detection of replica at network level. In this scheme, sub-areas can be scaled easily by dividing their angles. However, this scheme is subject to single-point of failure. Moreover the communication overhead is quite high in inter sub-area replica detection.

III. PROPOSED SYSTEM

In the proposed system an energy efficient ring based clone detection protocol (ERCD) protocol to achieve high clone detection probability with random witness selection, while ensuring normal network operations with satisfactory network lifetime of WSNs.

The ERCD protocol can be divided into two stages: witness selection and legitimacy verification

Developing the system construction model, to evaluate and implement the proposed system. In this module, we consider a network region with one base station (BS) and an enormous number of wireless sensor nodes randomly distributed in the network

The sink node is the origin of the system coordinator. Based on the location of the BS, the network region is virtually separated into adjacent rings, where the width of each ring is the same as the transmission range of sensor nodes. The network is a densely deployed WSN, i.e. for each node, there exist sensor nodes located in each neighbour ring and for each ring, in the each ring, there are enough nodes to construct a routing path along the ring.

By introducing the distributed clone detection protocol, namely ERCD protocol, which can achieve a high clone Detection probability with little negative impact on network lifetime and limited requirement of buffer storage

Capacity.The ERCD protocol consists of two stages: witness selection and legitimacy verification. In witness selection, a random mapping function is employed to help each source node randomly select its witnesses. In the legitimacy verification, a verification request is sent from the source node to its witnesses, which contains the private information

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 10, October 2018

of the source node. If witnesses receive the verification messages, all the messages will be forwarded to the witness header for legitimacy verification, where witness headers are nodes responsible for determining whether the source node is legitimacy or not by comparing the messages collected from all witnesses. If the received messages are different from existing record or all the messages are expired, the witness header will report a clone attack to the sink to trigger a revocation procedure.

PROBABILITY OF CLONE DETECTION

Designing a distributed clone detection protocol with random witness selection by jointly considering clone detection probability, network lifetime data buffer storage, Initially, a small set of nodes are compromised by the malicious user. maximizing the clone detection probability by Utilizing the clone detection protocol,, i.e. the probability that cloned node can be successfully detected, to ensure the security of WSNs In distributed clone detection protocol with random witness selection, the clone detection probability generally refers to whether witnesses can successfully transmitted from the source node to its witnesses.

ENERGY CONSUMPTION AND NETWORK LIFETIME

In WSNS, since wireless sensor nodes are usually powered by batteries, it is crucial to evaluate the energy consumption of sensor nodes and to ensure that normal network operations will not be broken down by node outage. Therefore, we define the network lifetime as the period from the start of network operation until any node outage occurs to evaluate the performance of the ERCD protocol.

We only consider the transmission power consumption, as the reception power consumption occupies little percentage of total power consumption. Since witness sets in our ERCD Protocol are generated based on ring structure, sensor nodes in the same ring have similar tasks. To simplify the analysis, we suppose that all sensor nodes in the same ring have some traffic load,

Our analysis in this work is generic, which can be applied to various energy models. A node inside (outside) ring k refers to the node which locates in the ring with the index smaller than (larger than) k. First, we analyze the traffic load of each sensor node, such that the energy consumption and network lifetime can be derived based on it. By using the ERCD protocol, traffic load of each sensor node consists of normal data collection, witness selection and legitimacy verification.

IV. EXPERIMENTAL SETUP

Python 2.7 version in UBUNTU is used to execute and run the program and other needed. Few packages of Python are being installed to get the accurate result.

V. RESULTS

Chooses the number of packets sent to the server and then the timer starts. The packets are sent and not if not, it will resend the packets when the timer starts. If the acknowledgement lost it will resent the packet after resending the packets it will receive the packets and the acknowledgement will be sent to the client

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 10, October 2018

Clients sending the packets are shown below

```
vinod@vinod-Inspiron-5558:~$ pwd routingproject
/home/vinod
vinod@vinod-Inspiron-5558:~$ cd routingproject
vinod@vinod-Inspiron-5558:~/routingproject$ python client.py GBN.txt 7780 10
|-|-|-|-|-|-|-|-|-| Sender info |-|-|-|-|-|-|-|-|-|
host: 127.0.0.1
protocol: GBN
Window size: 8
Timeout: 10
MSS: 30
Port: 7780
Number of packets to send: 9
Sending S0; Timer started
Sending S1; Timer started
Received ACK:  0Sending S2; Timer started

Sending S3; Timer started
Sending S4; Timer started
Sending S5; Timer started
Sending S6; Timer started
Sending S7; Timer started
Sending S8; Timer started
Timeout, sequence number = 1
Resending packet: S1; Timer started
Resending packet: S2; Timer started
Resending packet: S3; Timer started
Resending packet: S4; Timer started
Resending packet: S5; Timer started
Resending packet: S6; Timer started
Resending packet: S7; Timer started
Resending packet: S8; Timer started
Received ACK:  1
Received ACK:  2
Received ACK:  3
Timeout, sequence number = 4
Resending packet: S4; Timer started
Resending packet: S5; Timer started
Resending packet: S6; Timer started
Resending packet: S7; Timer started
Resending packet: S8; Timer started
Ack 4 lost (Info for simulation).
Timeout, sequence number = 4
Resending packet: S4; Timer started
```

Fig 1 Client.py

- **The detection of the clone is done. And the client sends the packets to the server for the acknowledgement.**

Choose the number of packets to be sent to the server and then the timer starts. The packets are sent and if not, it will resend the packets when the timer starts. If the Acknowledgment lost, the packets are resent and this is shown below:

```
Resending packet: S5; Timer started
Resending packet: S6; Timer started
Resending packet: S7; Timer started
Resending packet: S8; Timer started
Ack 4 lost (Info for simulation).
Timeout, sequence number = 4
Resending packet: S4; Timer started
Resending packet: S5; Timer started
Resending packet: S6; Timer started
Resending packet: S7; Timer started
Resending packet: S8; Timer started
Received ACK:  4
Received ACK:  5
Received ACK:  6
Received ACK:  7
Received ACK:  8
vinod@vinod-Inspiron-5558:~/routingproject$
```

Fig 2 client.py

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 10, October 2018

- **If the packets are not sent, then re-sending of packets can be done. And then the timer begins.**

```
vinod@vinod-Inspiron-5558:~$ pwd routingproject
/home/vinod
vinod@vinod-Inspiron-5558:~$ cd routingproject
vinod@vinod-Inspiron-5558:~/routingproject$ python server.py 7780 GBN 8
|-|-|-|-|-|-|-|-|-| Receiver info |-|-|-|-|-|-|-|-|-|
Hostname: 127.0.0.1
Port: 7780
Protocol: GBN
Packet received for S0
ACK sent for S0
Packet S1 lost. (Info for simulation)
Packet received for S2
(Packet out of order, discarded): last received packet in sequence: packet 0
Packet received for S3
(Packet out of order, discarded): last received packet in sequence: packet 0
Packet received for S4
(Packet out of order, discarded): last received packet in sequence: packet 0
Packet received for S5
(Packet out of order, discarded): last received packet in sequence: packet 0
Packet S6 lost. (Info for simulation)
Packet received for S7
(Packet out of order, discarded): last received packet in sequence: packet 0
Packet received for S8
(Packet out of order, discarded): last received packet in sequence: packet 0
Packet received for S1
ACK sent for S1
Packet received for S2
ACK sent for S2
Packet received for S3
ACK sent for S3
Packet S4 lost. (Info for simulation)
Packet received for S5
(Packet out of order, discarded): last received packet in sequence: packet 3
Packet received for S6
(Packet out of order, discarded): last received packet in sequence: packet 3
Packet received for S7
(Packet out of order, discarded): last received packet in sequence: packet 3
Packet received for S8
(Packet out of order, discarded): last received packet in sequence: packet 3
Packet received for S4
ACK sent for S4
Packet received for S5
ACK sent for S5
```

Fig.3 server.py

The server screen is shown below. It will receive the packets send by the client. After receiving the packets the acknowledgement will be sent to the client.

```
Packet received for S6
ACK sent for S6
Packet received for S7
ACK sent for S7
Packet received for S8
ACK sent for S8
Packet received for S4
ACK sent for S4
Packet received for S5
ACK sent for S5
Packet received for S6
ACK sent for S6
Packet received for S7
ACK sent for S7
Packet received for S8
ACK sent for S8
vinod@vinod-Inspiron-5558:~/routingproject$
```

Fig 4 Server.py

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 10, October 2018

Finally the packets are received to the server and acknowledgments are sent for the received packets to the client.

VI. CONCLUSION

We have proposed distributed energy efficient clone detection protocol with random witness selection. Specifically we have proposed the ERCD protocol, which includes the witness selection and legitimacy verification stages. Both of our theoretical analysis and simulation results have demonstrated that our protocol can detect the clone attack with most probability 1, since the witnesses of each sensor node is distributed in ring structure which makes it easy be achieved by verification message. In addition, our protocol can achieve better network lifetime and total energy consumption with reasonable storage capacity of data buffer. This is because we take advantage of the location information by distributing the traffic load all over WSNs, such that the energy consumption and memory storage of the sensor nodes around the sink node can be relieved and the network lifetime can be extended. In our future work, we will consider different mobility patterns under various Network scenarios.

REFERENCES

[1] Z. Zheng, A. Liu, L. X.Cai, Z. Chen, and X. Shen, "ERCD: An energy-efficient clone detection protocol in 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 emerging machine to machine communications," IEEE Communications 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 Energy Management Routing in WSN", International Journal of 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, "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. 2012.
[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] P. Papadimitratos, J. Luo, and J. P. Hubaux, "A randomized coun-termeasure against parasitic adversaries 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 effective strategy for location privacy in VANETs," IEEE Transactions 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 malicious activities for smart grid communications," IEEE Network, vol. 25, no. 5, pp. 50–55, May. 2011.
[10] R. Lu, X. Lin, X. Liang, and X. Shen, "A dynamic privacy-preserving key management scheme for location based services in VANETs," IEEE Transactions 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 wireless sensor networks," IEEE Transactions on Dependable and Secure Computing, vol. 8, no. 5, pp. 685–698, Sep.-Oct. 2011.
[12] Y. Zeng, J. Cao, S. Zhang, S. Guo, and L. Xie, "Random-walk based approach to detect clone attacks in wireless sensor networks," IEEE Journal on Selected Areas in Communications, vol. 28, no. 28, pp. 677– 691, Jun. 2010