International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 5 Issue: 5 1035 – 1039

Clone Detection for Efficient System in WSN using AODV

Prof. Roshani Talmale
M Tech III Sem
TGPCET, Nagpur

Ms. Rupika Yadav
Guide Co-guide
HOD, CSE
TGPCET, Nagpur

Prof. Vishal Tiwari
Co-guide
Dept. of CSE
TGPCET, Nagpur

***Abstract*—** Wireless sensor is wide deployed for a spread of application, starting from surroundings observance to telemedicine and objects chase, etc. For value effective sensing element placement, sensors are usually not tamperproof device and are deployed in places while not observance and protection, that creates them at risk of fully different attacks. As an example, a malicious user may compromise some sensors and acquire their private information. Then, it'll duplicate the detectors and deploy clones in an exceedingly wireless sensor network (WSN) to launch a spread of attack that's mentioned as clone attack. Because the duplicated sensors have an equivalent information, e.g., code and crypto graphical information, captured from legitimate sensors that may merely participate in network operation and launch attacks. Because of the low value for sensing components duplication and preparation, clone attacks became one in all the foremost essential security issues in WSNs. Thus, it's essential to effectively detect clone attacks therefore to ensure healthy operation of WSNs.

***Keywords*—** *Security attack, Base Station, Clone attack, Clone attack detection, Centralized approach, Distributed approach.*

*****

1. INTRODUCTION

1.1 Background

Wireless device Network (WSN), typically referred to as wireless sensor and mechanism network (WSAN), are spatially distributed autonomous sensors to watch physical or environmental conditions, like temperature, sound, pressure, etc. and at hand in glove pass their data through the network to a main location. The extra trendy network are bi-directional, additionally facultative management of sensing element activity. The event of wireless sensor network was intended by military application like field of battle surveillance; these days such network are used in many industrial and consumer application, like method observation, and so on.

A wireless sensor network is also a cluster of specialised transducers with a communications infrastructure for observation and recording conditions at varied locations. Usually monitored parameters are temperature, humidity, pressure, wind direction, illumination intensity, vibration intensity, sound intensity, power-line voltage, chemical concentrations, pollutant levels and very important body functions.

Clustering is one among the necessary strategies for prolonging the network lifespan in wireless sensor networks (WSNs). It involves grouping of sensor nodes into clusters and electing cluster heads (CHs) for all the clusters. CHs collect the information from several cluster's nodes and forward the collective data to base station. A significant challenge in WSNs is to pick applicable cluster heads. In this paper, we have a tendency to present a fuzzy decision-making approach for the choice of cluster heads. Fuzzy multiple attribute decision-making (MADM) approach is employed to pick CHs using 3 criteria together with residual energy, variety of neighbors, and also the distance from the base station of the nodes. The simulation results demonstrate that this approach is more practical in prolonging the network lifespan than the distributed hierarchical agglomerative clustering (DHAC) protocol in homogenous environments.

In several situations, the information collected by several nodes are same. In such cases, redundant information transmission are often eliminated by forming group of nodes known as clusters and by electing one node among the nodes within the cluster to be cluster head. All nodes will send information to the cluster head wherever the aggregation of information will takes place. There are 2 kinds of clustering techniques. The clustering technique applied in homogenous sensor networks is termed homogeneous clustering schemes, and also the clustering technique applied within the heterogeneous sensor networks is stated as heterogeneous clustering schemes. If we've used mounted node as the cluster head, then it's to gather information from all of its child nodes and needs to process the information for all the period of time. This results in quicker battery evacuation within the mounted cluster head. Although one cluster head dies, it'll affect the working of the network. By selecting dynamic cluster head, this drawback are often eliminated.

 ISSN: 2321-8169
1035 – 1039

The two basic approaches for the co-ordination of entire clustering method are distributed and centralized. In distributed clustering, wherever every sensor node will run their own algorithmic rule and takes the choice of turning into cluster head. In centralized clustering, a centralized authority teams the nodes to make clusters and cluster heads. Generally hybrid theme may be enforced.

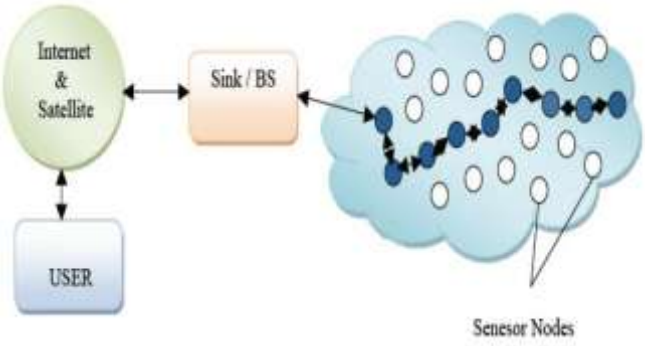


Figure 1: General Overview of Wireless Sensor Networks

1.2 Our contribution

In this paper, besides the clone detection chance, we additionally think about energy consumption and memory storage within the style of clone detection protocol, i.e., an energy- and memory-efficient distributed clone detection protocol with random witness choice scheme in WSNs.

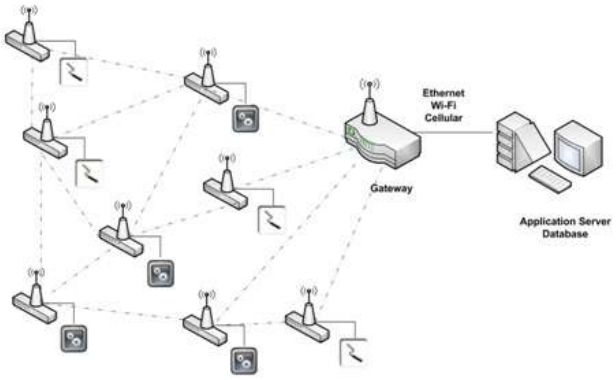
Our protocol is applicable to general densely deployed multi-hop WSNs, wherever adversaries might compromise and clone sensor nodes to launch attacks.

We extend the analytical model by evaluating the desired information buffer of ERCD protocol and by including experimental results to support our theoretical analysis. Energy-Efficient Ring primarily based Clone Detection (ERCD) protocol.

We find that the ERCD protocol will balance the energy consumption of sensors at completely different locations by distributing the witnesses everywhere WSNs except non-witness rings, i.e., the adjacent rings around the sink, that shouldn't have witnesses.

After that, we acquire the optimum range of non-witness rings based on the perform of energy consumption.

Finally, we derive the expression of the desired information buffer by using ERCD protocol, and show that our projected protocol is ascendable because the desired buffer storage depends on the ring size only.



2. Related Work

One of the first solutions for the detection of node replication attacks depends on a centralized base station [15]. During this resolution, every node sends a list of its neighbors and their claimed locations (i.e., the geographic coordinates of every node) to a Base Station (BS). Identical entry in 2 lists sent by nodes that aren't "close" to each other can end in clone detection. Then, the bs revokes the clones. This resolution has many drawbacks, like the presence of one point of failure (the BS), and high communication prices due to the massive range of messages. Further, nodes near the bs are needed to route much more messages than other nodes, thus shortening their operational life.

Other solutions have faith in local detection. As an example, in [13, 14, 15, 16] a vote mechanism is employed within an area to agree on the legitimacy of a given node. However, applying this type of technique to the matter of duplicate detection, fails to discover clones that aren't among a similar neighborhood. As delineated in [19], a naïve distributed resolution for detecting the node replication attack is Node-To-Network Broadcasting. With this resolution every node floods the network with a message containing its location data and compares the received location data therewith of its neighbors. If a neighbor s_w of node s_a receives a location claim that a similar node s_a is during a position not coherent with the position of s_a detected by s_w, this may lead to the detection of a clone. However, this technique is extremely energy intense since it needs n floodings per iteration, wherever n is that the variety of nodes within the WSN

3. Sensor network model

3.1. Network topology

We adopt the same network model as [20, 22]. The network consists of n uniform sensors arbitrarily and uniformly distributed over a target. Events occur uniformly specified each sensor has one packet to report sporadically. The neighboring distance is outlined because the highest approachable distance of radio frequency with the utmost transmission power. Every sensor may be conscious of this energy state of its neighbors and also the energy needed to

transmit information from every of its neighboring sensors to the base station [23]. We assume an ideal transmission model, i.e., a sensor's neighbors will receive all the messages that the sensor transmits. Once a sensor transmits a message to at least one of its neighbors or the base station, the sensor attaches the data of its remaining energy to the message so that all of the neighbors will update its energy state. This updating method guarantees that data of neighboring sensors for the routing call is obtainable for sensors. The lifespan of the network is that the time advance until the primary sensor node within the network uses up its energy. The goal is to maximize the network lifespan by planning an energy-efficient routing algorithm.

3.2. Energy consumption model

Sensors consume energy when they are sensing, receiving and transmitting [24]. The quantity of energy consumed for sensing isn't associated with routing [25]. Therefore, we tend to think about only the energy usage for sending and receiving messages. In line with the radio model employed in [21], energy consumption for sending is given by Eq. (5)

$$\begin{cases} E_{mem} = lE_{elec} + l\varepsilon_{fs}d^2 & if\ d < d_0 \\ E_{mem} = lE_{elec} + l\varepsilon_{amp}d^4 & if\ d > d_0 \end{cases} \quad (5)$$

where Eelec is sending circuit loss. Each the free area (d^2 power loss) and the multi-path attenuation (d^4 power loss) channel models are considered within the model, betting on the space between sender and receiver. $\mathcal{E}f_s$ and $\mathcal{E}_{amp}$ are the energy needed by power amplification in these two models, resp. The energy spent for receiving an l-bit packet is

$$E_R(l) = lE_{ele} \quad (6)$$

The above parameter settings are given in Table 1 [21].

Table 1
Network Parameter

Parameter	Value
Threshold distance (d0) (m)	87
Sensing range rs (m)	15
Eelec (nJ/bit)	50
efs (pJ/bit/m2)	10
eamp (pJ/bit/m4)	0.0013
Initial energy (J)	0.5

4. ERCD PROTOCOL

Here, we tend to introduce our distributed clone detection protocol, named as ERCD protocol, which may accomplish a high clone detection probability with very little negative impact on network lifespan and restricted demand of buffer capability. The ERCD protocol consists of two stages: witness selection and legitimacy verification. In witness selection, a random mapping perform is utilized to assist every source node arbitrarily choose its witnesses. Within the legitimacy verification, a verification request is sent from the source node to its witnesses, which contains the non-public info of the source node. If witnesses receive the verification messages, all the messages will be forwarded to the witness header for legitimacy verification, wherever witness headers are nodes liable for determining whether or not the source node is legitimacy or not by scrutiny the messages collected from all witnesses. If the received messages are totally 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.

5. Proposed Routing Algorithm

The protocol relies on On-demand ad hoc routing protocol (AODV).Brief description of techniques is given here

Ad hoc On-Demand Distance Vector (AODV):

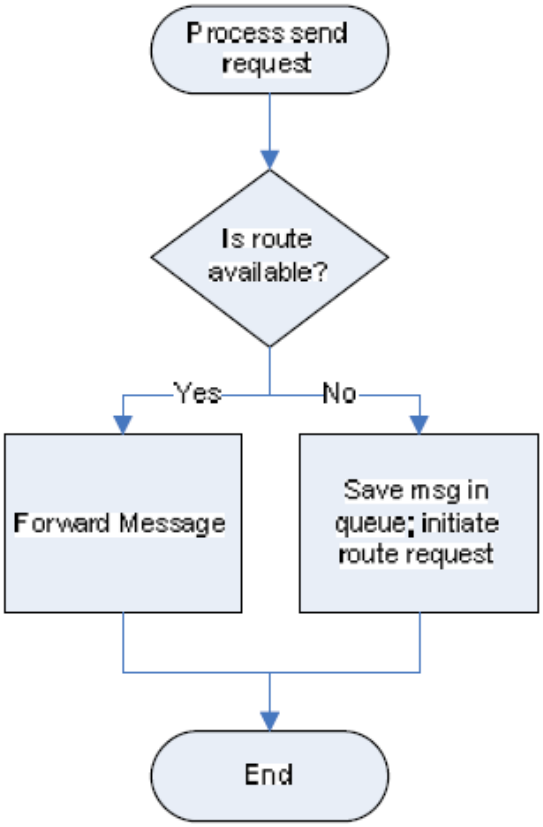
The ad hoc On-Demand Distance Vector (AODV) routing protocol is meant to be used by mobile nodes in an ad hoc network. It offers fast adaptation to dynamic link conditions, low process and memory overhead, low network utilization, and determines unicast routes to destinations among the ad hoc network. It uses destination sequence numbers to confirm loop freedom the least bit times (even within the face of abnormal delivery of routing control messages), avoiding issues (such as "counting to infinity") related to classical distance vector protocols.

Each AODV router is basically a state machine that processes incoming requests from the SWANS network entity. Once the network entity has to send a message to a different node, it calls upon AODV to see the next-hop. Whenever an AODV router receives a request to send a message, it checks its routing table to check if a route exists. Every routing table entry consists of the subsequent fields:

- Destination address
- Next hop address
- Destination sequence number
- Hop count

If a route exists, the router merely forwards the message to subsequent hop. Otherwise, it saves the message in a message queue, then it initiates a route request to determine a route. The subsequent flow chart illustrates this process:

 ISSN: 2321-8169
1035 – 1039



Figure

Upon receipt of the routing info, it updates its routing table and sends the queued message(s).

AODV nodes use four varieties of messages to communicate among one another. Route Request (RREQ) and Route Reply (RREP) messages are used for route discovery. Route Error (RERR) messages and hello messages are used for route maintenance.

CONCLUSION

In this paper, we have projected distributed energy-efficient clone detection protocol with Ad-hoc on demand distance vector. An ad Hoc On-Demand Distance Vector (AODV) could also be a routing protocol designed for wireless and mobile ad hoc networks. This protocol establishes routes to destinations on demand and supports every unicast and multicast routing. We have an inclination to profit of the location information by distributing the traffic load all over WSNs, nominative the energy consumption and memory storage of the device nodes round the sink node. In our future work, we'll take into consideration fully totally different quality patterns beneath varied network situations.

Acknowledgment

The authors would really like to CSE Department and Principal of TGPCET Tulsiram Gaiyakwad Patil college of Engineering & Technology providing their support and facilities like labs, software's etc. needed to carry out this work.

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, 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," IEEE Commun.Mag., vol. 49, no. 4, pp. 28–35, Apr. 2011.

[3] A. 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," Comput. Netw., vol. 56, no. 7, pp. 1951–1967, May. 2012.

[4] T. Shu, M. Krunz, and S. Liu, "Secure data collection in wireless sensor networks using randomized dispersive routes," IEEE Trans. Mobile Comput., vol. 9, no. 7, pp. 941–954, Jul. 2010.

[5] P. Papadimitratos, J. Luo, and J. P. Hubaux, "A randomized countermeasure against parasitic adversaries in wireless sensor networks," IEEE J. Sel. Areas Commun., vol. 28, no. 7,pp. 1036–1045, Sep. 2010.

[6] 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 Trans. Veh. Technol., vol. 61, no. 1, pp. 86–96, Jan. 2012.

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

[8] R. Lu, X. Lin, X. Liang, and X. Shen, "A dynamic privacy-preserving key management scheme for location based services in VANETs," IEEE Trans. Intell. Transp. Syst., vol. 13, no. 1, pp. 127–139, Jan. 2012.

[9] M. Conti, R. D. Pietro, L. Mancini, and A. Mei, "Distributed detection of clone attacks in wireless sensor networks," IEEE Trans.Dependable. Secure Comput., vol. 8, no. 5, pp. 685–698, Sep.-Oct. 2011.

[10] M. Conti, R. D. Pietro, L. Mancini, and A. Mei, "Distributed detection of clone attacks in wireless sensor networks," IEEE Trans.Dependable. Secure Comput., vol. 8, no. 5, pp. 685–698, Sep.-Oct. 2011.

[11] Y. Zeng, J. Cao, S. Zhang, S. Guo, and L. Xie, "Random-walk based approach to detect clone attacks in wireless sensor networks,"IEEE J. Sel. Areas Commun., vol. 28, no. 28, pp. 677–691, Jun. 2010.

[12] B. Zhu, S. Setia, S. Jajodia, S. Roy, and L. Wang, "Localized multicast: Efficient and distributed replica detection in large-scale sensor networks," IEEE Trans. Mobile Comput., vol. 9, no. 7, pp. 913–926, Jul. 2010.

[13] H. Chan, A. Perrig, and D. Song. Random key predistribution schemes for sensor networks. In *Proceedings* of 2003 IEEE Symposium on Security and Privacy (S&P *'03)*, pages 197–213, 2003.

ISSN: 2321-8169
1035 – 1039

[14] J. R. Douceur. The sybil attack. In *Proceedings of the 1st* International Workshop on Peer-to-Peer Systems (IPTPS *'01)*, pages 251–260. Springer, 2002.

[15] L. Eschenauer and V. D. Gligor. A key-management scheme for distributed sensor networks. In *Proceedings of the 9th* ACM Conference on Computer and Communications *Security (CCS '02)*, pages 41–47, 2002.

[16] J. Newsome, E. Shi, D. Song, and A. Perrig. The sybil attack in sensor networks: analysis & defenses. In *Proceedings of ACM IPSN'04*, pages 259–268, 2004.

[17] Y. Xuan, Y. Shen, N. P. Nguyen, and M. T. Thai, "A trigger identification service for defending reactive jammers in WSN," IEEE Trans. Mobile Comput., vol. 11, no. 5, pp. 793–806, May. 2012.

[18] R. Lu, X. Lin, H. Zhu, X. Liang, and X. Shen., "BECAN: A bandwidth-efficient cooperative authentication scheme for filtering injected false data in wireless sensor networks," IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 1, pp. 32–43, Jan. 2012.

[19] B. Parno, A. Perrig, and V. D. Gligor. Distributed detection of node replication attacks in sensor networks. In Proceedings of 2005 IEEE Symposium on Security and *Privacy (S&P '05)*, pages 49–63, 2005.

[20] C.-S. Ok, S. Lee, P. Mitra, S. Kumara, Distributed energy balanced routing for wireless sensor networks, Comput. Ind. Eng. 57 (1) (2009) 125–135.

[21] W.R. Heinzelman, A. Ch, H. Balakrishnan, Energy-efficient communication protocol for wireless microsensor networks, in: Proceedings of the 33rd Hawaii International Conference on System Sciences,2000.

[22] C-S. Ok, S. Lee, P. Mitra, S. Kumara, Distributed routing in wireless sensor networks using energy welfare metric, Inform. Sci. 180 (2010) 1656–1670.

[23] IEEE.802.11, Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification, IEEE std. 802.11-1999 ed., 1999.

[24] Q. Wang, W. Yang, Energy consumption model for power management in wireless sensor networks, in: 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Network (SECON'2007), 2007, pp. 142–151.

[25] M. Stemm, R.H. Katz, Measuring and reducing energy consumption of network interface in hand-held devices, IEICE Trans. Commun. E80-B (8) (1997) 1125–1131.