Spam Detection and Recovery Model for WSN

Ashish Kumar Srivastava, Aditya Goel, Jyoti Srivastava

Abstract: Wireless sensor network (WSN) is susceptible to various kinds of security attacks; one among them which is more prevalent is DoS(Denial of Service) attack. Spam message consumes most of the node energy and cause energy constraints node to drain with energy. So the prevention of such kind of attack is required in WSN. To solve this issue we are using a systematic approach of identifying spam message which may lead to the DoS attack. We are using a set of mobile agents which perform specifically assigned task to control overflow of excess Spam messages so as to stop DoS attack. The proposed spam prevention model for the MA(Mobile Agent) is experimented on WSN. The proposed model Restrict the unnecessary MA's roaming and cloning are minimized and thus the energy can be saved. To calculate the threshold value we have used two techniques; one is based on the number of itinerary the clone threshold is set and the other is based on the simple moving average method so as to calculate the threshold value for the number of remote MA's. Based on the previous threshold values the new threshold value is calculated. The analysis shows that as the node is increasing from 1 to 10 how drastically Anti MA's clone generated in when DADR model is not used and how the number reduces when DADR model is used. Subsequently energy is saved by applying DADR model. Through this proposed model DoS attack detection and Recovery Model (DADR), we can avoid the spam attack in the WSN. This proposed model named as DADR (DoS attack detection and recovery) is proposed. Simulation results validate this DADR model which is able to stop spreading of anti-MA. This stop unnecessary energy drains of sensor nodes and also allows normal agent operations in the WSN. The principle behind this proposed DADR model is to restrict the unauthorized mobile agent for conserving the processing energy of sensor nodes.

II. BASIC DOS ATTACK MODEL

The special features of sensor nodes like its self-organizing capability, continuous sensing, cooperative effort, etc make it a very powerful technology in almost all WSN applications scenario. Multi-hop communication consumes less power than traditional single-hop network which is an important requirement for WSN. Some of the spam attack and code injection attack is elaborated in [1], [5], [6] and [7]. For efficient WSN environment, we need to prevent spam MA attack. Our model focuses on the hazard of anti MA attack and a novel prevention MA model to mitigation. Fig. 1 shows the DoS attack from Anti MA. In this spam request generation model, the attacker sensor node will continuously send spam anti MA's to all the other sensor nodes in the network and also to the BS. Due to these spam anti MA's, the regular working of sensor node becomes impossible. Due to the continues dispatch of Anti MA through some compromised sensor node or some malicious node as in diagram the center sensor node sending anti MA causes hindrance in the normal functioning of WSN. Due to the SPAM attack the genuine MA could note able to access the network resources.

Fig. 1: Spam Agent attack
The rest of the paper is organized as follows: Section 2 gives the problem definition Section 3 presents proposed DADR model. Section 4 presents results and discussion of proposed model. Section 5 gives conclusion of the proposed model.

1. Problem Definition

Spam based DoS attack is one of the unsolved research issue, which may be attempted in two different ways given below:

i. By injecting anti MA sensor nodes into existing WSN
ii. By injecting anti MA programs into any existing sensor nodes of WSN

Anti MA is a silent spam attack which dispatches malicious code into sensor nodes of WSN where it continuously replicates to generate clones anti MAs. These cloned anti MAs send sensed data to the BS and stay inside sensor nodes to consume its resources. Thus spam based DoS attack can exhaust the resource constraints WSN node. Signal jamming attack is a more successful form of DoS attack against a WSN as shown in [3].

2. DOS Attack Detection and Recovery (DADR) Model

Malicious or anti MAs are software program which are programmed with malicious intention. Life cycle of an anti MA and its attacking scenario is elaborated in Fig. 2. It shows spam attack scenario, here insertion of anti MA program is assumed to be done in two ways one is by injecting through remote sensor node and another by injecting through anti sensor node. This created clone is migrated to neighboring node and from neighboring nodes data is sent repeatedly like spam. The proposed DADR model has three types of module. The functions of each module are described below:

a) Planner Mobile Agent (PMA): PMA waits for a MA to check authentication. It keeps track of existing MAs with the help of Agilla middleware and it will be fired after reaching at a particular threshold. It also keeps track on memory consumption inside WSN nodes. Other features include such as register reaction for AMA (Approve Mobile Agent) and QMA (Quarantine Mobile Agent) and changing its state from sleeping to working mode and vice versa.

b) Approve Mobile Agent (AMA): AMA can be invoked when authenticated MAs are injected and it will be fired after exceeding the threshold limit. Then it kills all MAs inside sensor nodes or selects a MA that contained maximum clones according to instructions for managing a space to the newly injected MA, after that it will go into sleeping or waiting mode.

c) Quarantine Mobile Agent (QMA): QMA can be invoked when unauthenticated MAs are injected or new clones are created inside sensor nodes. After crossing threshold limit, it will get fired. Once QMA is fired, it clears all clones and their resources before sending PMA to sleep mode.

The proposed model is designed to restrict the transmission of anti MAs that may be either authorized or unauthorized. This will reduce the overhead on sensor nodes. The proposed model may pre exist inside the sensor nodes or can be injected from outside, when needed in the WSN environment. Proposed model is simulated using a robust middleware named Agilla to inject the MA on TinyOS platform, TOSSIM to make the WSN environment and PowerTOSSIM to measure the power in WSN environment.

Proposed DADR model is divided into three phase, which is described in flowchart in Fig. 3. First phase starts with the initial setup of WSN environment, where PMA will be installed at each sensor nodes. We assume that first phase completed within setup time of WSN and consumed energy will not be added while evaluating our model. We also assume that our proposed DADR model is most of the time in waiting mode and they are invoked as required on each sensor node till their lifetime or before removing PMA from that sensor node.

After PMA setup phase, the second phase will start when new agent is injected in any sensor node of WSN otherwise it remain in sleeping mode. Here we assume that PMA has been set to $GMA_{\text{max}} = r$ while $QMA_{\text{max}} = s$. In sensor node 1, we assumed that there are five MAs as well as 10 clones are created. After receiving any MA, PMA is fired and checks for its authentication. For authenticated MA, PMA fires AMA when MAs exceed $GMA_{\text{max}}$, let say ($GMA_{\text{max}} = 5$) otherwise it allows MA to work in sensor node 1. Now for this sixth injected authenticated MA, QMA makes a space for it by killing a MA inside sensor node1 which created maximum clones say or it may delete all MAs. For unauthenticated MAs, PMA fires AMA when MAs exceed $QMA_{\text{max}}$ ($QMA_{\text{max}} = 10$). Now AMA clears all clones and their consumed

![Fig.2: Spam Anti Mobile Attack Scenario](image)
memory in the sensor node 1. At the end, the sensor node 1 comes into sleeping mode. Third phase deals with calculation of threshold value of $GMA_{max}$ and $QMA_{max}$ so that spam attack can be avoided and recovered. To calculate threshold value we have used simple moving average (SMA). The algorithm of the proposed DADR model is given in Fig no.4. Injected anti MA initially creates its own clones and migrate clone to all neighbor sensor nodes one by one as shown in Fig. no.2. This results into spreading of anti MA throughout WSN. They will stay inside sensor node permanently and consume resources such as CPU, Memory, energy, radio total, etc.

After migrating anti MA to all neighbor sensor nodes, every host sensor node sends data to the BS. The data may consist of the various possible parameters such as temperature, power status, host ID, agent ID, etc. In this attacking scenario each sensor node may exists $w \times (w-1)/2$ clones, which stay inside sensor node permanently and consume resources [4]. A mathematical equation for rejection of MAs request in a sensor node can be given as:

$$\sum_{i=1}^{w} POW_{\text{con}} + SPW_{\text{con}} + COM_{\text{pow}} = P_{\text{total}}$$

(5.1)

Or

$$\sum_{i=1}^{w} MEM_{\text{con}} + DEF_{\text{con}} = M_{\text{total}}$$

(5.2)

Where:

- $POW_{\text{con}}$: Power consumed during migration from one sensor node to another
- $SPW_{\text{con}}$: Power consumed per iteration for sending data
- $MEM_{\text{con}}$: Memory consumed per anti MA
- $P_{\text{total}}$: Total battery power
- $M_{\text{total}}$: Total memory space
- $COM_{\text{pow}}$: Computational power taken by each sensor node for anti MA
- $DEF_{\text{con}}$: Default memory space for other applications
- $w$: Number of anti MA iterations

Threshold calculation for clones: In this attacking scenario maximum number of MA’s clone i.e. $N^2$ will be created, where $N$ is the number of sensor nodes in a WSN. All clones are using sensor nodes resources and create hazard for WSN. The proposed model enables to prevent the spread of anti MAs and now maximum $2 \times N$ clones will be created. The comparison of maximum number of clones created by spam MAs and our proposed model for 10 sensor nodes in the WSN is mentioned in Table 1.

Table 1: Number Of MA’s Clones Generated During Spam Attack.

| Sensor nodes | Anti MA’s clone generated in Without DADR model | MA’s clone generated in With (DADR) |
|--------------|-----------------------------------------------|------------------------------------|
| 1            | 1                                             | 1                                  |
| 2            | 4                                             | 4                                  |
| 3            | 27                                            | 6                                  |
| 4            | 256                                           | 8                                  |
| 5            | 3125                                          | 10                                 |
| 6            | 46656                                         | 12                                 |
| 7            | 823543                                        | 14                                 |
| 8            | 1677726                                       | 16                                 |
| 9            | 387420489                                     | 18                                 |
| 10           | 10000000000000                                | 20                                 |

Threshold calculation for clones and MA: We have used the simple moving average (SMA) method to calculate the threshold value [8]. Normally to setup the threshold value in SMA, we need to consider the previous scenarios. For example what is the frequency of flow of MAs and generation of clones in sensor nodes at the time of...
Spam Detection and Recovery Model for WSN

deployment? Based on this we have to set the threshold value.

The threshold value for this spam prevention is calculated using eq. (5.3) and (5.4) which will use the

average of the last \( x \) data (threshold value) to calculate the current data (threshold value).

\[
THV_j = \frac{\sum_{i=1}^{x} p_i}{x}
\]

(5.3)

Where:

\( p_i \): Number of incoming MAs in the sensor node on \( i^{th} \) day or duration

\( THV_j \): Threshold value of the \( j^{th} \) day or duration

\( x \): Number of days or duration considered for the SMA

To determine the value \( p_i \), the Eq. (5.4) is used.

\[
p_i = \frac{\sum q_i^{m-1}}{m}
\]

(5.4)

Where \( q_i \) is the number of MA request sent by the \( i^{th} \) sensor node and \( m \) is the number of sensor node sent the MA. Table 5.2 shows the procedure for calculating the threshold value \( TV \) using the Eq. (5.3) and (5.4). In case any sensor node sends the MA more than \( TV \) then it will get blocked, similar case for the cloning of the MAs.

III. RESULTS AND DISCUSSION

We assume that PMA exist inside every sensor node in WSN and consumed equal amount of energy to fire PMA and to handle AMA & QMA. We will inject MAs to fire PMA at sensor node 1. Therefore we calculate total energy in sensor node 1. Fig.4 illustrates that number of MA’s clone generated are reduced drastically by applying proposed model and thus it is resolving the spam attack.

Fig.4: Anti mobile agent clones generated for spam attack and proposed model

Table 3 indicates the energy consumed by spam MA attack during 5 different simulations at sensor node 1.

Table 3: Energy consumed during spam attack without DADR

| Simulation | Energy consumption in spam Attack With MA (mJ) | Energy consumption in initial setup (mJ) |
|------------|----------------------------------------------|----------------------------------------|
| S1         | 2004.779                                     | 1707.312                               |
| S2         | 2093.101                                     | 1756.176                               |
| S3         | 2084.025                                     | 1749.539                               |
| S4         | 2085.981                                     | 1769.959                               |
| S5         | 2043.499                                     | 1772.751                               |

As we have assumed that the energy consumed in initial setup of proposed model is not considered for the analysis so the actual energy taken for spam attack model is give as: Actual mean energy taken by spam attack model without DADR =2062.277-1751.147=311.131

Table 3 indicates the energy consumption of proposed DADR model during 5 different simulations at sensor node
Table 4: Energy consumed during spam attack with DADR

| Simulation | Energy consumption for handling malicious MA (mJ) | Energy consumption for Initial setup of Proposed Model (mJ) |
|------------|-----------------------------------------------|-------------------------------------------------|
| S1         | 1950.197                                      | 1900.145                                        |
| S2         | 2011.577                                      | 1863.873                                        |
| S3         | 2030.224                                      | 1921.396                                        |
| S4         | 2048.245                                      | 1812.801                                        |
| S5         | 1848.941                                      | 1862.728                                        |
| Average    | 1977.8368                                     | 1872.189                                        |

As we have assumed that the energy consumed in initial setup of proposed model is not considered for the analysis so the actual energy taken for proposed DADR model is given as:

Actual mean energy taken for spam attack with proposed DADR model
=1977.8368 - 1872.189 = 102.117

Consumed energy in the simulation of proposed model, spam attack at sensor node 1 is listed in Table 4 and their comparing graph in shown in Fig.5

Fig.5 : Average energy consumed

IV. CONCLUSION

When a WSN is compromised by attacker and this compromised node sends its MA very frequently to all neighboring nodes to share its dummy or public key then DoS attack will happen. If the compromised sensor node frequently sends its MA to the neighbor sensor nodes then the number of transmissions and reception will increase which will lead to the consumption of radio energy of the sensor nodes. If it continues then all the sensor nodes will die after a period of time and it will bring into the DoS. To overcome this issue a novel MA spam attack detection and recovery model is proposed named as DoS attack detection and recovery (DADR) model to control spam anti MA based DoS attack. Simulation results validate this DADR model which is able to stop spreading of anti-MA and thus reducing the energy and time consumption; hence appropriate for WSN environment. The analysis shows that as the sensor node is increasing from 1 to 10 how drastically Anti MA’s clone generated when DADR model is not used and how the number reduces when DADR model is used. Subsequently 50% of energy is saved by applying DADR model. Through this proposed model DoS attack detection and Recovery Model (DADR), we can avoid the spam attack in the MA based wireless sensor environment and save energy of resource constraints WSN and hence increase its life.

REFERENCES

1. Anthony D. Wood and John A. Stankovic, “Taxonomy for Denial-of-Service Attacks in Wireless Sensor Networks”, Computer, 35(10) pp 54-62:2002.
2. David R. Raymond and Scott F. Midkiff, “Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses” Published by the IEEE CS, 2008 IEEE.

3. Aristides Mpitziopoulos and Damianos Gavalas, “An effective defensive node against jamming attacks in sensor networks,” in Security And Communication Networks. (2008) Published online in Wiley InterScience (www.interscience.wiley.com) DOI: 10.1002/sec.81.

4. Ashish Kumar Srivastava et al., "MASAP: Mobile Agent Spam Attack Prevention for WSN Environment," in International Conference on Computational Intelligence and Information Technology, Pune, India, 2011 © Springer LNCS, vol.250, part 2, pp.450-452.

5. V. Coskun et al., “Quarantine region scheme to mitigate spam attacks in wireless-sensor networks,” IEEE Trans. On Mobile Computing, vol. 5, no. 8, pp. 1074-1086, Aug 2006.

6. Bai Li and Lynn Batten, “Using mobile agents to recover from node and database compromise in path-based DoS attacks in wireless sensor networks,” Journal of Network and Computer Applications, pp. 377–387, 2009.

7. Aurélien Francillon et al., “Code Injection Attacks on Harvard Architecture Devices”, 2008 © ACM. DOI: 978-1-59593-810-7/08/10.

8. Weisstein and Eric W, "Spencer's 15-Point Moving Average." From MathWorld—A Wolfram Web Resource. http://mathworld.wolfram.com/Splencers15-PointMovingAverage.html.

9. B. D Lange and M Oshima, "Seven good reasons for mobile agent communication of the ACM, vol.42, no.3, pp.98-89, 2001.

Dr. Ashish Kumar Srivastava did his B.E. in Electrical and Electronics Engineering from Bharatiyar University Coimbatore Tamil Nadu, and M.Tech in Information Technology from Tezpur Central University Assam. He has completed his Ph.D in Information Technology, in the area of security issues in wireless sensor network from MANIT Bhopal (Deemed University). He has teaching research and Administrative experience of more than 17 years from various Institutes and universities. He has published more than 25 Research papers in reputed International Journals & Conferences including IEEE, Springer. His areas of interests are wireless Communication, Information security, Cyber Security.

Dr. Aditya Goel did his B.E. (Hons) in Electronics & Communication and M.Tech in Communication Engineering from I.I.T. Bombay. Subsequently he was awarded with the Ph.D. degree in Electronics & Communication Engineering in the Year 2000. He has teaching & research experience of more than 20 years. Presently he is working as Associate Professor in the Deptt. of Electronics & Communication Engineering at Maulana Azad National Institute of Technology(Deemed University), Bhopal, India. He has published more than 70 Research papers in reputed International Journals & Conferences including IEEE. His areas of interests are Optical Communication, Digital Signal Processing, Optical Networks, Computer Communication etc. He has guided several M.Tech dissertations and Ph.D thesis on these areas. He had been Principal Investigator of the research project titled “ BroadBandLlightwave communication systems” sanctioned by Govt. of India, New Delhi. Presently also he is working as Principal Investigator of the R&D Project “ High speed optical components for WDM systems” sanctioned by M.H.R.D. Govt. of India, New Delhi. He has reviewed many research papers of International conferences & journals including SPIE. He is a Life Fellow member of the Institution of Electronics & Telecommunication Engineers and Senior Member of Computer Society of India.

Dr. Jyoti is working as a Sr. Assistant Professor in Madanapalle Institute of Technology and Science, Madanapalle, Andhra Pradesh. Jyoti has completed her M.Tech and PhD from IIIT Allahabad as a TCS Research Scholar. She has received the “Mahindra all India talent scholarship” by “KC Mahindra Education Trust” of Mahindra and Mahindra Ltd.” during 3 year diploma in Electronics Engineering. She has total 4 years of experience out of which 2 years of research and industrial experience and 2 years of teaching experience.