ISSN 2277-3061

COMPRO-MOTO: An efficient approach for identifying compromised nodes in wireless sensor networks

[1st] Vinayaka S.N, [2nd] M Dakshayini
[1st] Department of Information Science and Engineering, BMS College of Engineering,Bangalore
vinayakasnvinni8@gmail.com
[2nd] Professor,Department of Information Science and Engineering, BMS College of Engineering,Bangalore
dakshayini.ise@bmsce.ac.in

ABSTRACT

Wireless sensor networks (WSNs) are exposed and being attacked by opponents as they are randomly deployed in open environments. Opponents can extract confidential information like secret keys by inserting their own nodes as compromised nodes and uses them to introduce various security attacks. So detection of such nodes is being the major issue to be addressed. In this paper we present Compro-Moto – as an efficient intrusion detection system to detect compromised nodes in WSNs. Simulation results clearly shows the benefits of Compro-Moto :(i). It is not sensitive to any kind of security attacks (ii).It endows detection range up to 99.99%. (iii)It endows false detection rate less than 1%in WSNs.(iv).It endows less total overhead and less packet loss rate. These benefits are the achievement of Compro-Moto system that requires little memory and less communication overhead and also it can scale up to millions of nodes.

Indexing terms/Keywords

Wireless sensor networks (WSNs); Compro-Moto; compromised node; Intrusion detection system and Status-Line.

ISSN 2277-3061

1. INTRODUCTION

The sensor nodes are very cheap; due to this it has allowed WSNs to be extensive used in many areas like health care and traffic control so on. However security is more important concern in WSNs.

The nodes in the WSNs have little memory, little power consumption and their battery life is also little, so WSNs can be deployed in open environments. Therefore they get exposed to opponents quickly. If intruder's nodes are not detected then it becomes authorized nodes of the deployed network. Later with this acquisition they start to introduce various kinds of security attacks.Thus security plays a vital role in WSNs, hence we need to think of various security measures for prevention, detection and recovery. Here the nodes are inexpensive and their resource limitations can hinders effectiveness of prevention[1,2,3]. So opponents can easily acquire nodes through systems and other hacking techniques.

Several approaches exists to identify acquired nodes, but they all have some sort of drawbacks and some are very poor in providing required security [3,4].

In this paper we present a Compro-Moto, a new intrusion detection system to find out compromised nodes in WSNs

(i).It endows 99.99% faultless in detecting compromised nodes within detection range.

(ii). It is not specific to a single application, whereas it can be used for all type of deployment with respect to compromised node detection

(iii).Our algorithm each time it encounters the behavior of every node to detect its mischievousness in order to provide the system robustness.

(iv)Using this technique the resources can be scale up and down with minimum computational overhead.

(v).It serves 99.99% false detection rate.

Rest of the paper is structured as follows: section 2 discusses Literature Survey, section 3 describes Compro-Moto's design in detail, section 4 explains simulation work, Part-V shows Simulation Results .Lastly, Part-VI Concludes and discusses future work

2. LITERATURE SURVEY

An earlier method of detection system makes use of several software-based attestation techniques. These techniques only identify the nodes which are mischief but it doesn't provide any feature to drop compromised nodes [6, 7, 8]. There are several Compromised node identification approaches like Replication [5, 9], Wormhole [10] [11], and Sybil [12] [13].These approaches are very specific and moreover here opponents can easily suppress the detection mechanisms

Several approaches are there for detecting mischief node based on rule-based and anomaly-based like COOL but they consider only identification for outgoing traffic not incoming traffic[14]. For example, Onat and Miri proposed an intrusion detection system (IDS) that monitors two features: (1) the packet arrival rate and (2) the receive power [20]. Nodes will continue to monitor these two features from neighbors and any new value that deviates a certain amount from the established baseline is considered anomalous. Malicious behavior that causes a change in either feature, such as a replay attack, would be detectable. Rule-based approaches detect misbehavior as soon as a condition, established before deployment of the network, is met. For example, COOL is an IDS that uses the relationship between incoming and outgoing messages to detect compromised nodes . COOL's approach is based on the observation that the majority of outgoing messages should be forwards of incoming messages. Any node that is sending T more than it is receiving, where T is some threshold, is considered to be compromised.

Our work differs from several other approaches in terms of Correctenesss, Elasticity, and Fault-Tolerant. It equips a good intrusion detection system to provide more security with less computational overheads and it never allows any opponents to hinder the activity carried out inside the detection system.

3. COMPRO-MOTO'S DESIGN

The architecture of Compro-Moto's is shown in Figure.1. This technique Comprises of two important elements they are: (i) Dispersed Element (ii) Unified Element.

The dispersed element run on each and every node where as the unified element runs on head node i.e. Base station in WSNs.Dispersed Element-element runs on every node in order to supervise the decency of adjacent or closest nodes as shown in Figure.2.With less communication overhead by checking the sender/Receiver packet rate.Unified Element-Here, the head node is used to collect the data from the whole network through network analysis. Head node consists of Compro-Moto detection system, that decides whether the node is compromised or not based on report generated by intrusion system.

Sections 3.1 and 3.2 discusses dispersed and unified Element in detail.

3.1. Dispersed Element:

Initially, each and every node is set up with some standard parameters like Sensor Data, Sender/Receiver Power Rate, Sending Data Rate and Receiving Data Rate. These are called as Status-Line. It records data from all adjacent nodes and stores in its own Message buffer.

ISSN 2277-3061

During communication each and every node evaluates recently recorded data to check whether its adjacent node has violated its Status-Line. If it is deviated from Status-Line then such node is termed as mischief node and report the same to the head node

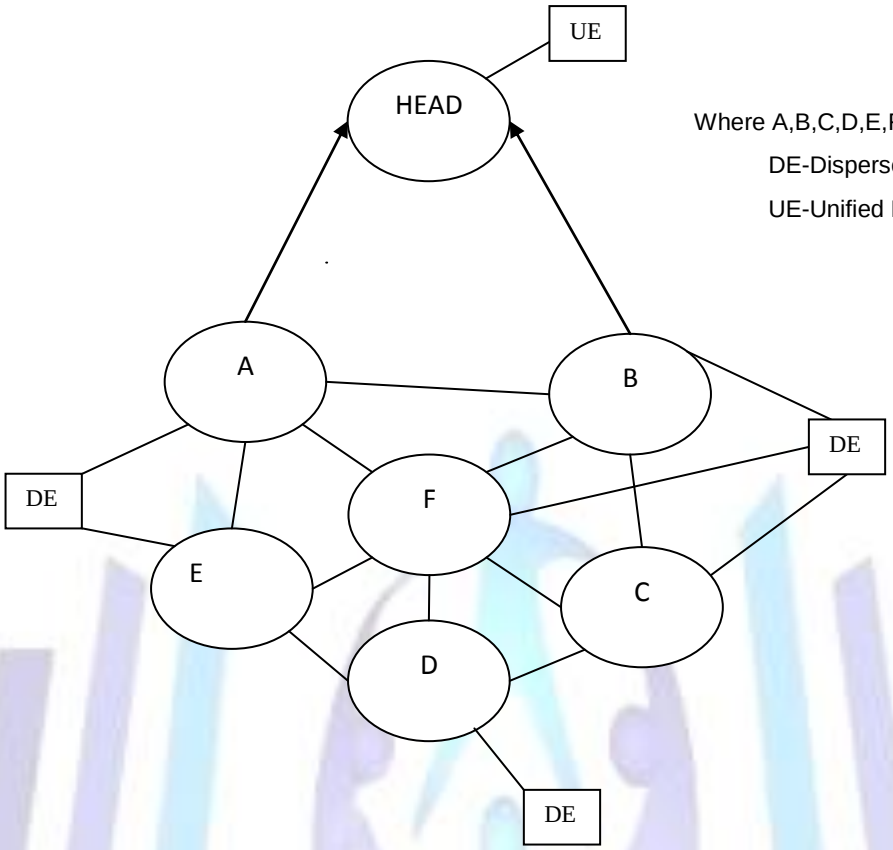

Figure 1 Compro-Moto's Architecture

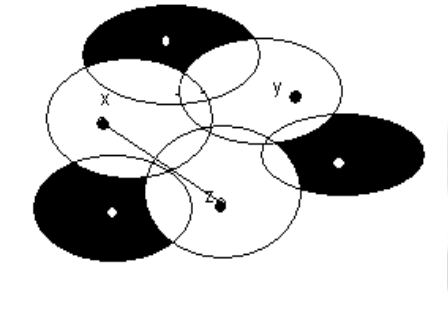

Figure 2 Node x supervises Node Z

Some of the features are

- Sensor Data: The readings of one node are not dependent of that of its adjacent. By supervising the sensor data, we can detect attacks that attempt to interrupt collected information.
- Sender/Receiver Power Rate: In static networks, the receiver/sender power rate should remain constant. variations in a power may be caused by changes in the communication hardware or position of the corresponding node.
- Sending Data Rate: Most of the applications senses the data and transmit them periodically. Data packets should be routed periodically. Thus the rate of packets sent by nodes follow a consistent pattern.
- Receiving Data Rate: The ratio between incoming and outgoing packets should be constant because outgoing packets can only be packets being routed or packets generated by the node.

Two different proposed procedures to detect compromised nodes are Error-Based procedure and Strict-Based procedure. In Error-Based procedure a Status-Line is established from the collected data and any new collected data that differ from the Status-Line are to be treated as errors. In Strict-Based procedure it checks for a specific condition.

Our Compro-Moto is divided into seven Modules. First module is of Sensor Data, Second is of Sender/Receiver Power Rate. Third is of Sending Data Rate, Fourth is of receiving Data Rate, Fifth is of joining messages from various nodes,Sixth is of Rabin-Pair wise and Random key distribution algorithm in order to provide security[15,16,17,18].

The first four belongs to Error-Based and the last two are Strict –Based. For the Strict-Based if a node detects a new adjacent node after a set up period by hearing any messages from that new node will be treated as compromised node.

3.1.1 Error-Based Procedure

Every node has two buffers; they are Message buffer and the Mischief Buffer. These buffers are shared by all first four modules and use a sliding window approach. When the Last M messages/reports about the corresponding adjacent nodes are stored. The Data stored in the message buffer is used to estimate the adjacent Status- Line. New messages are compared against the Status-Line and any messages that violate from the Status-Line and by more than certain levels are to be treated as Errors. Those Erroneous messages are treated as Mischief's and cause the identifying node to generate Mischief Report. All such reports are added to its Mischief Buffer. If such behavior happens to be continuous, it crosses above Status-Line then such node will be report to head node.

The following formula is used to estimate Sender/Receiver Power Rate

$pow_{new} - pow_{max} > P$, if $pow_{new} > pow_{max}$

$pow_{min} - pow_{new} > P$ $pow_{new} < pow_{min}$ (1)

Where, pow_{new} – New Power Rate,

pow_{min} - Minimum Power Rate,

pow_{max} - Maximum Power Rate,

P - Power Status-Line

The above formula estimates minimum and maximum values of Message receiver/Sender power rate from the message buffer. A new packet is erroneous if its receiver/sender power rate is P below the min or P above the max. Any identified erroneous packets are considered to be mischiefs. Erroneous packets are added to the message buffer, so that errors caused by environmental changes can be accounted in future Status-Line estimations.

The Procedure that uses the sensor data is almost identical to the one that uses the receiver/sender power rate. The only difference is that the difference between the node's and the adjacent sensor data is used instead of the receiver/sender power rate as shown below in Figure.3.

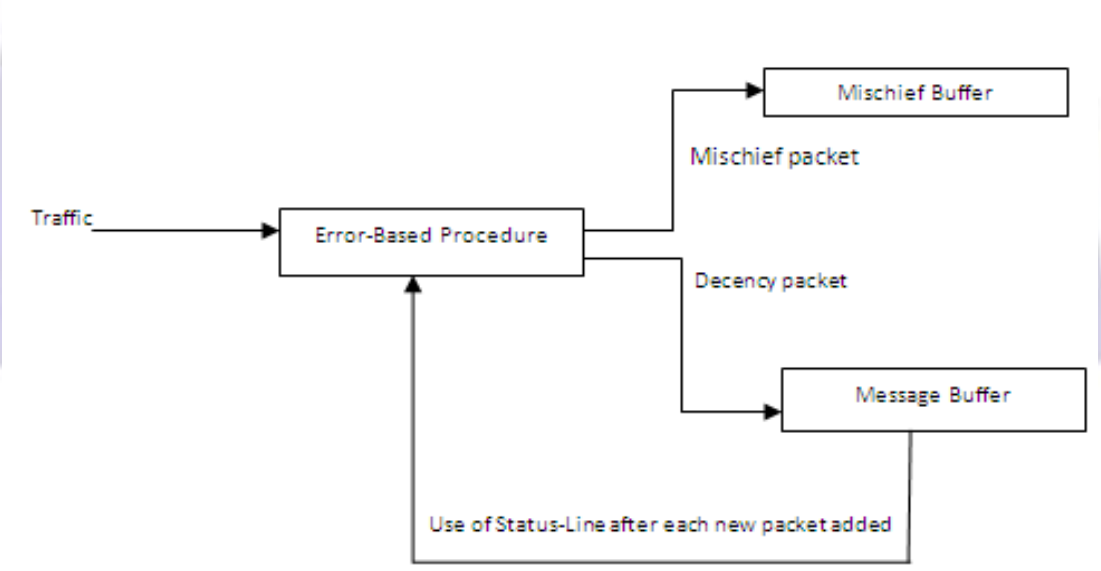

Figure 3 Identification algorithms which makes use of sender/receiver power and sensor data.

Figure.4 shows an overview of the Procedure that uses the sending data rate. It calculates two rates: the rate at which the last M2 messages are sent (including the last message), $rate_{M2}$, and the rate at which the last M messages are sent, $rate_M$ where M > M2. If the ratio of these two rates is above a Status-Line D the corresponding adjacent is considered to be acquired. Where, D- DataRate Status-Line.

ISSN 2277-3061

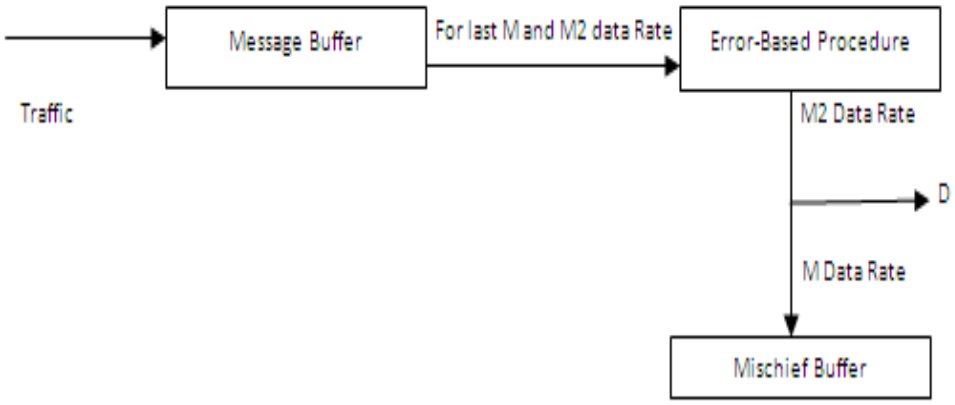

Figure 4 Identification algorithms which makes use sending data rate and receiving data rate

The algorithm that uses the receive rate differs in two ways. First, instead of computing messages sent by the neighbor, the counts of packets received from the neighbor (i.e., sent to the adjacent)can be cosidered. Second, the rates are replaced with send-receive ratios (i.e., $rate_{M2}$ becomes $ratesent_{M2}$=$raterec_{M2}$ and $rate_{M}$ becomes $ratesent_{M}$ /$raterec_{M}$).

3.2. UNIFIED ELEMENT:

The Unified Element running on the head node is responsible for ensuring that, weather the reported node is really compromised or not. This decision is made by considering data collected rom other nodes. If the reported node is desided as compromised, the head node will alert all the user and perform required recovery procedures like deleting all of its messages. However, if the reported node is desided as not truly compromised node, then the head node intimate all the reporter(s) to treat it as non-compromised and continue supervising.

3.2.1 Strict-Based Procedure

Here the head node will process data based on reports from other nodes. In order to make a decision about whether a reported node is compromised, Compro-Moto uses a Gamma probabilistic theory. It has been shown that Gamma probabilistic theory is able to correctly detect mischievous node based on numerous reports and lower the false Detection rates in strict detection systems because the system takes history into account, Gamma Probabilistic theory are an extension that uses probability density functions to combine feedback from multiple sources and determine a reputation rating, or rating of how trustworthy the subject node is. In our case, the reputation rating corresponds to a decision of compromised or not if it is past a threshold value.

In Gamma probabilistic theory, the probability p is a reported event and is accurate with respect to given two parameters α and β distribution. f(ρ|α,β) can be expressed using the gamma function r as:

$$f(\rho|\alpha,\beta) = \frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)+\Gamma(\beta)}\rho^{\alpha-1}(1-\rho)^{\beta-1}, \quad 0 \le \rho \le 1, \alpha > 0, \beta > 0 \tag{2}$$

We chose the parameters, α and β, to be the weighted sum of past reports for the reported node and the number of compromised nodes within two hops of the reported node. These allow the network topology and past reports to impact the final decision about whether a reported node is compromised. Initial StatusLine values are determined during the setup period.The head node has knowledge of every node's neighbor, which may have been gathered during the setup period. X report about node X being compromised by node Y has a higher probability of being correct the more of nodeX's neighbor's report it, the longer its history of reported, and the more compromised nodes there are near it.

On the other hand, if the probability is too low, then the reporter node Y, may be compromised and launching a slander attack against node x. In which case, the head node will instruct other nodes that node Y is compromised, alert the user, and launch recovery procedures.

This approach prevents opponents from using Compro-Moto to attack the network without being detected. If a compromised node impersonates the head node, nodes closer to the head node on the routing path will detect messages coming from the wrong direction and alert the head node Thus, an opponent cannot spoof the head node without being immediately detected.

ISSN 2277-3061

4. IMPLEMENTATION

The proposed Compro Moto algorithm has been simulated using ns-2 simulator. Standard library files like libcap and libstd and trusted packages 2.26 are used. There were two key issues that may be applicable to other implementations of Compro-Moto.

First, recall that every node has a mischief buffer for each of its supervised adjacent. The format and size of that buffer is implementation-dependent (i.e., depends on the needed correctness and performance evaluation of the WSN).

Secondly, there may be a high memory overhead for the buffers need to supervise all adjacent. The overhead grows as a quadratic function of the number of immediate adjacent, which is not scalable for high density networks. To address this, Compro-Moto nodes can select a subset of adjacent to supervise. The selection can be random or come from other protocols. For example, in random pair-wise key distribution protocols and Rabin algorithm [15][16][17][18], there are a number of keys generated before deployment and each node is given a random key. After deployment, there is a probability that two neighboring nodes will have compatible keys and be able to communicate. Depending on the density of the network. it's possible to control the average number of neighbors that each node can communicate with it by adjusting the total number of keys.

5. SNAPSHOTS AND RESULTS

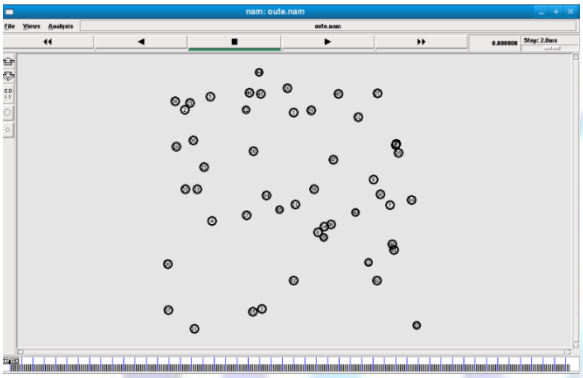

Figure 5 Initially nodes are placed

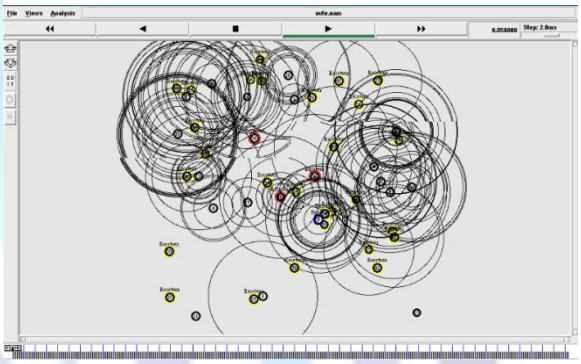

Figure 6 Opponents Introduce Its Attacker Node

Initially nodes are placed and set up with initial values (Status-Line) as shown in figure 5. After a while, during communication intruders may introduce their node as shown in figure6 (red Nodes)

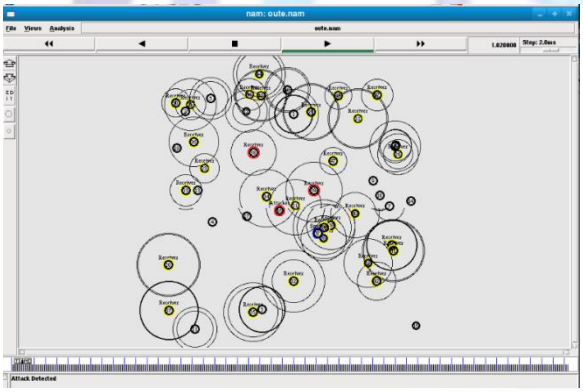

Figure 7 Attack detected

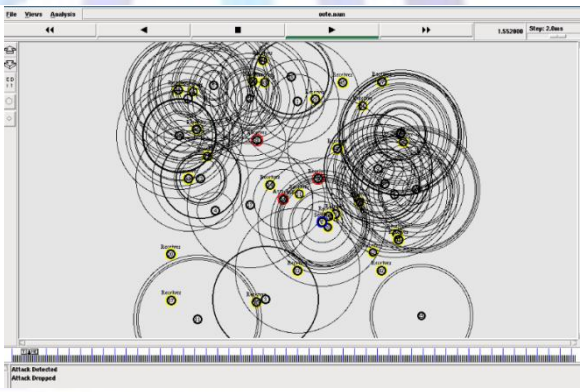

Figure 8 Attack dropped

By executing Compro-Mote algorithm the compromised nodes are detected and dropped as shown in figure 7 and figure 8 respectively. Periodical event generation is shown in figure 9. Simulation results of detection overhead in shown figure 10 and total communication overhead in shown in figure 11. Finally False detection rate is as shown in figure 12.

ISSN 2277-3061

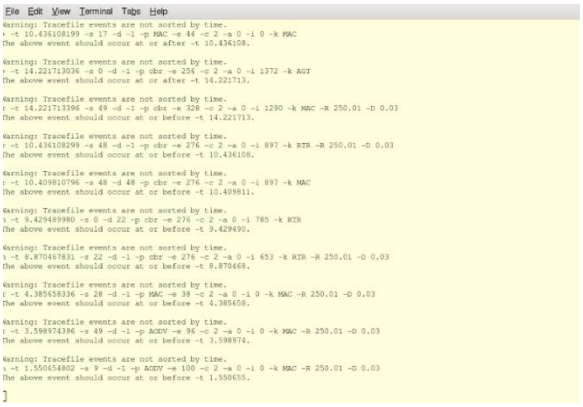

Figure 9Traffic event generation

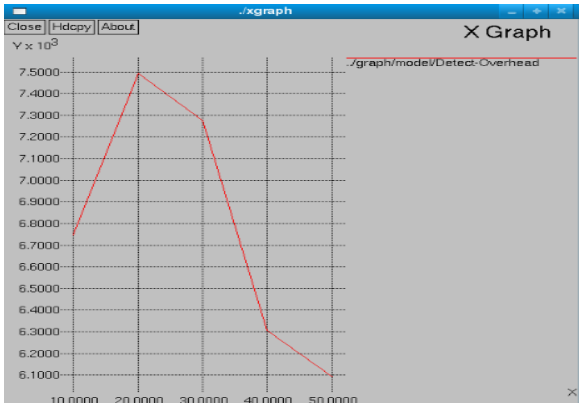

Figure 10 Detection Overhead

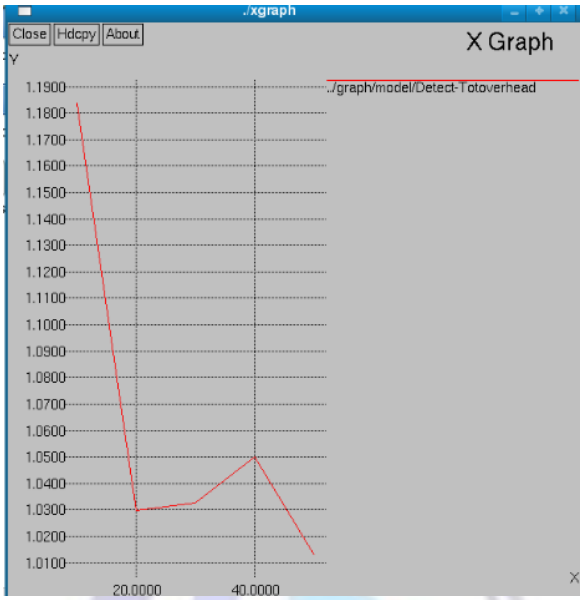

Figure 11 Total overhead

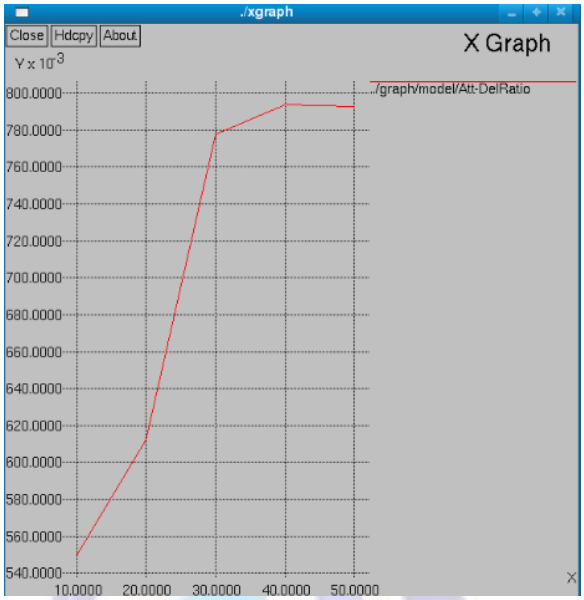

Figure 12 False detection

6. CONCLUSION

In WSNs undetected compromised nodes may destroy the integrity of data by sending false data reports, injecting false data, and disrupting transmissions. Since cryptographic solutions are not sufficient to prevent these attacks, we proposed Compro-Moto algorithm, a system for detecting compromised nodes in WSNs.

Compro-Moto algorithm has been proved as an efficient intrusion detection system to detect compromised nodes in WSNs. Simulation results clearly shows the benefits of Compro-moto :(i). It is not sensitive to any kind of security attacks(ii).It endows detection range up to 99.99%. (iii)It endows false detection rate less than 1%in WSNs.(iv).It endows less total overhead and less packet loss rate. Such benefits cannot be achieved by other systems which are existing today. This system requires little memory and less communication overhead due to this it can scale up to millions of nodes. Possible directions for future work include creating a response system and adding a challenge system.

ACKNOWLEDGMENTS

The authors would like to acknowledge and thank Technical Education Quality Improvement Program [TEQIP] Phase 2, BMS College of Engineering and SPFU [State Project Facilitation Unit], Karnataka for supporting the research work.

REFERENCES

[1] C. Castelluccia, A. Francillon, D. Perito, and C. Soriente. On the difficulty of software-based attestation of embedded devices. In CCS '09: Proceedings of the 16th ACM conference on Computer and communications security, pages 400–409, New York, NY, USA, 2009. ACM.

[2] C. Krau, M. Schneider, and C. Eckert. On handling insider attacks in wireless sensor networks. Information Security Technical Report,

[3] X. Chen, K. Makki, K. Yen, and N. Pissinou. Node compromisemodeling and its applications in sensor networks. In Computers and Communications, 2007. ISCC 2007. 12th IEEE Symposium on, pages 575–582, July 2007.

[4] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. A survey on sensor networks. Communications Magazine, IEEE, 40(8):102 – 114, Aug2002.

[5] M. Conti, R. Di Pietro, L. V. Mancini, and A. Mei. A randomized, efficient,and distributed protocol for the detection of node replication attacks in wireless sensor networks. In Proceedings of the 8th ACM international symposium on Mobile ad hoc networking and computing, MobiHoc '07,pages 80–89, New York, NY, USA, 2007. ACM.

[6] A. Seshadri, M. Luk, and A. Perrig. Sake: Software attestation for key establishment in sensor networks. In DCOSS '08: Proceedings of the 4th IEEE international conference on Distributed Computing in Sensor Systems, pages 372–385, Berlin, Heidelberg, 2008. Springer-Verlag.

[7] A. Seshadri, M. Luk, A. Perrig, L. van Doorn, and P. Khosla. Scuba: Secure code update by attestation in sensor networks. In WiSe '06:Proceedings of the 5th ACM workshop on Wireless security, pages 85–94, New York, NY, USA, 2006. ACM.

[8] A. Seshadri, A. Perrig, L. V. Doorn, and P. Khosla. Swatt: oftwarebasedattestation for embedded devices. In In Proceedings of the IEEESymposium on Security and Privacy, 2004.pages 188–200, New York, NY,USA, 2004. ACM.

[9] B. Parno, A. Perrig, and V. Gligor. Distributed detection of node replicationattacks in sensor networks. In Security and Privacy, 2005 IEEE Symposium

[10] Y.-C. Hu, A. Perrig, and D. Johnson. Packet leashes: a defense against wormhole attacks in wireless networks. In INFOCOM 2003. Twenty- Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies, volume 3, pages 1976 – 1986 vol.3, Mar 2003

[11] S. Ganeriwal and M. B. Srivastava. Reputation-based framework for high integrity sensor networks. In In SASN 04: Proceedings of the 2nd ACMworkshop on Security of ad hoc and sensor networks, pages 66–77. ACMPress, 2004.

[12] M. Demirbas and Y. Song. An rssi-based scheme for sybil attack detection in wireless sensor networks. In Proceedings of the 2006 International Symposium on on World of Wireless, Mobile and Multimedia Networks, WOWMOM '06, pages 564–570, Washington, DC, USA, 2006. IEEEComputer Society.

[13] N. James, E. Shi, D. Song, and A. Perrig. The sybil attack in sensor networks: analysis & defenses. In Proceedings of the 3rd international symposium on Information processing in sensor networks, IPSN '04, pages.

[14] Y. Zhang, J. Yang, W. Li, L. Wang, nd L. Jin. An authentication scheme for locating compromised sensor nodes in wsns. J. Netw. Comput. Appl.

[15] R. Di Pietro, L. V. Mancini, and A. Mei. Random key-assignment forsecure wireless sensor networks. In Proceedings of the 1st ACM workshopon Security of ad hoc and sensor networks, SASN '03, pages 62–71, New York, NY, USA, 2003. ACM.

[16] D. Djenouri, L. Khelladi, and A. Badache. A survey of security issues in mobile ad hoc and sensor networks. Communications Surveys Tutorials,IEEE, 7(4):2 – 28, 2005.

[17] W. Du, J. Deng, Y. S. Han, P. K. Varshney, J. Katz, and A. Khalili. Apairwise key predistribution scheme for wireless sensor networks. ACMTrans. Inf. Syst. Secur., 8:228–258, May 2005.

[18] X. Du and H.-H. Chen. Security in wireless sensor networks. WirelessCommunications, IEEE, 15(4):60 –66, Aug 2008.259–268, New York, NY, USA, 2004. ACM.Spector, A. Z. 1989. Achieving application requirements. In Distributed Systems, S. Mullender

Author' biography

Mr. Vinayaka S N is a PG Scholar in Computer Networks and Engineering at B.M.S College Of Engineering, Bangalore. His research areas are Cloud Computing and Its security, Computer network.

Dr.M Dakshayini holds M.E and Ph.D degree in computer science and Engineering. She has more than one and a half decades experience in teaching field. She has taught many subjects in computer science field. She has published many research papers in refereed International conferences and Journals. Currently she is working as professor in the department of Information science and engineering at BMS College of Engineering, Bangalore, India.