Node Compromise Detection Based on Parameter Grouping in Wireless Sensor Networks

Manyam Thaile, O. B. V. Ramanaiah
Dept. of CSE, JNTUH College of Engineering
Hyderabad, Telangana State, India
e-mails: {manyamthaile, obvramanaiah}@gmail.com

***Abstract*—Node Compromise Detection (NCD) is an essential requirement for dealing with potential attacks in randomly deployed, unattended and not tamper resistant wireless sensor networks applications. Behaviour based concepts, such as false information communication by a compromised node (ZoneTrust), are reported in literature. In our work, more effective parameters, namely, packet sending rate, depletion of node energy, node location, and node non-availability are identified for NCD. All these parameters are used to detect a compromised node either conjunctively (AND model) or disjunctively (OR model). The OR model is suitable for military surveillance; and the AND model is suitable for weather monitoring applications. The OR model incurs a lot of overhead whereas the AND model suffers from high risk of attack. To alleviate these demerits Parameter Grouping (PG) concept is proposed to retain the merits of both AND and OR models. An extensive NS-2 based simulation work was carried out and found that the proposed NodeTrust-based PG improves the system performance substantially.**

***Keywords*—node compromise detection; software attestation; parameter grouping; wireless sensor network security**

I. INTRODUCTION

A Wireless Sensor Network (WSN) consists of a large number of sensor nodes, which perform sensing, processing and communication. There are different types of WSN applications, i.e., smart home security, battlefield surveillance, civil structure condition monitoring, crop pest control, etc. The sensor nodes have constrained resources such as limited battery energy, low computing power and low memory.

An attacker can easily capture the sensor nodes and compromise them due to the vulnerabilities of the sensor networks, i.e., unattended nature, low computing power (incapability to run software-based security concepts), lack of tamper-resistant hardware and unreliable communication, etc.

The node compromisation is a serious security threat to all WSN applications, because when a node is compromised, an attacker can launch a variety of attacks and inject malicious code. A compromised node is a trusted node (benign node) that has been taken control over by an attacker [8]. An attacker can compromise a sensor node in two ways:

- An attacker can physically capture a sensor node, connect it to a high-end computing system, steal the security keys, inject the malicious code, and thereby making the node compromised.
- An attacker can logically (remotely) connect a sensor node to high-end computing system, steal the secret keys, and inject the malicious code to make the node compromised.

To mitigate the damage incurred by compromised nodes, the system should detect and revoke the nodes at the earliest [12]. For addressing these issues, researchers have recently proposed various node compromise detection schemes, as well as revokation techniques. There are two approaches for handling Node Compromising [9], namely, prevention schemes, and detection schemes, as shown in Figure 1.

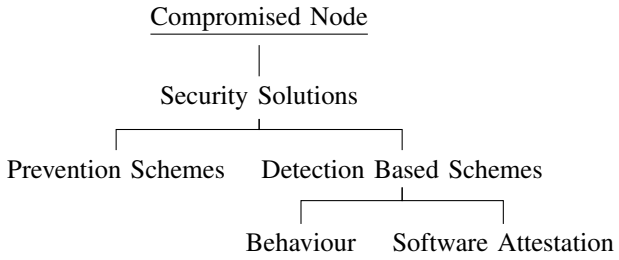

Figure 1. Security Solutions for Compromised Nodes.

Jun-Won Ho et al. [1] proposed a scheme named *ZoneTrust (ZT)* based on the concept of trust of a zone. If a zone is untrusted, then the base station applies the software attestation for each and every node in the zone. The drawbacks of this approach are:

- It is necessary for the base station to communicate with each and every sensor node of the untrusted zone which results in high communication overhead.
- Software attestation is applied on every node in the untrusted zones, in which some of the nodes are not compromised. This leads to computation overhead.
- Due to communication and computation overheads, ZoneTrust scheme consumes a lot of energy of the nodes.
- ZoneTrust considered only one parameter to determine untrusted zone, that is, false information communication.

In our previous work, packet arrival time (odd time of arrival) is used to detect a compromised node [14].

This paper proposes a better scheme with minimal overhead called *Parameter Grouping (PG)*. It identifies the untrusted nodes based on the five identified parameters of the behavior based approach, namely, packet sending rate, node energy depletion, node location, false information and non-availability of sensor nodes. Then, base station applies software attestation

 ISBN: 978-1-61208-493-0

on those identified nodes to decide the compromised nodes. Afterwards it revokes them immediately.

The rest of paper is organized as follows: Existing literature on NCD is reviewed in Section II. Network model, as well as attacker model are discussed in Section III. Section IV elaborates our proposed scheme (Parameter Grouping). Section V presents the simulation results. Finally, the paper concludes with Section VI.

II. Related Work

The prevention-based techniques are the first approach of defense for protecting sensor nodes using cryptography. The encryption and authentication are the primary measures in a prevention-based technique, based on key management, as that introduced in the security framework SPINS [7]. However, in case the first approach of defense is broken the compromised nodes could extract security-sensitive information (e.g., secret key), leading to breaches of security.

Thus, developing detection-based techniques as the second approach of defense has become of paramount importance. Detection based techniques aim at identifying misbehaviour and to check integrity of software. Detection based techniques are divided into two major categories as shown in Figure 1: Behaviour based and Software attestation based schemes.

The Behaviour based schemes detect misbehaviour of sensor nodes based on different parameters. For example, packet arrival time, packet arrival rate, packet sending rate, node location, node energy, etc. [5][6][11]. These techniques detect only misbehaviour, but fail to check integrity of malicious code.

The software-attestation based techniques have been proposed to detect the malicious code of sensor nodes. Specifically, the base station checks whether the flash image codes have been maliciously altered by performing attestation in randomly chosen portions of image codes or the entire codes [2][3][4]. These techniques detect only malicious code, but fail to detect misbehaviour of sensor nodes. The security architecture of wireless sensor networks [13] is shown Figure 2. The vertical comparison given in Figure 2 indicates that the various WSN security issues are addressed in every layer of the protocol stack from physical to application layers.

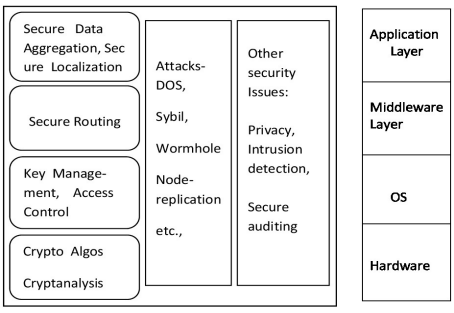

Figure 2. Security Architecture for WSN.

III. System Model

A. Network Model

The sensor network considered for our study is a static network in which a sensor node does not change its location once deployed. Besides, it is assumed that the base station is a trustworthy node. The communication between a sensor (leaf) node and base station takes place in two levels: from sensor node to Zone Head (ZH), and from ZH to base station. It is assumed that in every zone a sensor node nearest to base station is named as ZH. The proposed architectural model is depicted in Figure 3.

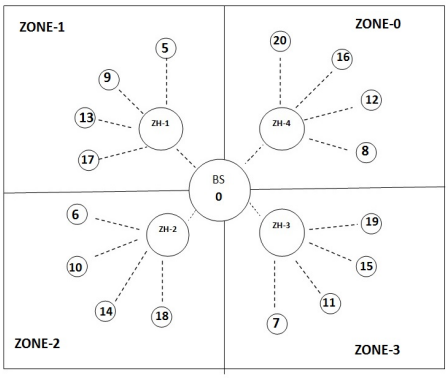

Figure 3. Architecture of Wireless Sensor Network.

B. Attacker Model

We assume that an attacker attempts to compromise as many nodes as possible in each zone. An attacker physically captures sensor nodes or remotely accesses them, compromises them, and re-deploys them back at different locations.

The attacker injects malicious code in all the captured nodes. This results in high packet sending rate, as well as faster depletion of compromised node's energy. The compromised nodes will be unavailable for the duration of the attack injection. Hence, it is to be noted that certain parameter values change unexpectedly.

C. AND-OR Model

The AND-OR Model estimates the trust of sensor nodes based on the behavioural parameters such as packet sending rate, depletion of node energy, node location, false information and non-availability of a node.

The evaluation of five parameters is follows:

- PSR (Packet Sending Rate): It can take different values, namely, HIGH, LOW, and NORMAL. If this parameter has value HIGH, then it is considered as satisfied (i.e., true).
- DNE (Depletion of Node Energy): It takes three values, namely, LOW, NORMAL, and HIGH. If DNE is equivalent to HIGH, then it is considered as true.
- NL (Node Location): Two values are possible, namely, Changed, and Unchanged. If NL is equivalent to Changed, then it is considered as true.

 ISBN: 978-1-61208-493-0

- FI (False Information): Two values are possible, namely, TRUE, and FALSE. If a node reports/communicates False Information, then the value of FI parameter is set to TRUE; else FALSE.
- NAN (Non Availability of Node): It takes two values, namely, YES and NO. If a node sends information periodically to ZH, it indicates its availability in the WSN; then NAN is set to NO; otherwise, YES.

The AND model identifies a node as untrustworthy, if it satisfies all the above five parameters simultaneously. In other words, the node is declared as untrustworthy when the conjunction of the five parameters is true. If at least one parameter is not true, then that node is not declared as untrust.

A node where all the identified parameters are valid/satisfied is declared as untrusted. Some (not all) parameters may be satisfying at each and every node of the network; and it might be the case that some nodes are already compromised. But the AND model does not detect these compromised nodes because all the parameters are not satisfying at those compromised nodes. Obviously, this model increases the vulnerability of the network for attacks (i.e., High risk).

The condition of AND model to be verified at i^{th}node is C_i=$(PSR_i \wedge DNE_i \wedge NL_i \wedge FI_i \wedge NAN_i)$. Node Status, NS is defined as follows:

$$NS(Node_i, TimeInterval_k) = \begin{cases} Untrust, if(C_i == True) \\ Trust, else \end{cases} \quad (1)$$

where PSR: **P**acket **S**ending **R**ate, DNE: **D**epletion of **N**ode **E**nergy, NL: **N**ode Location, FI: **F**alse **I**nformation and NAN: **N**on-**A**vailability of **N**ode.

The OR model categorizes a node as untrusted, which satisfies at least one of the above mentioned five parameters. In other words, the node is declared as untrusted when the disjunction of the five parameters is true. If all the parameters are not satisfied simultaneously, then only a node is declared as trust.

When more and more parameters are identified for NCD, only some (not all) parameters may be satisfied in case of a large number of nodes. As per OR Model, these nodes, where at least one parameter is valid, are identified as untrustworthy. This increases the number of nodes to be applied the software attestation to decide whether they are really compromised or not (Even if one parameter is satisfied by a node, it calls for software attestation for compromised node detection). This increases the software attestation overhead for OR model.

The condition of OR model to be verified at i^{th}node is C_i=$(PSR_i \vee DNE_i \vee NL_i \vee FI_i \vee NAN_i)$. Node Status, NS is defined as follows:

$$NS(Node_i, TimeInterval_k) = \begin{cases} Untrust, if(C_i == True), \\ Trust, else \end{cases} \quad (2)$$

The main motivation of Parameter Grouping is to strike the balance between risk of attack and attestation overhead. The OR model has a main advantage of low risk, whereas the AND model has the chief advantage of low overhead. To retain the merits of both, it is required to combine the two approaches. One way to achieve this is to group the parameters based on some criteria. Then, apply OR model among the groups, and the AND model within each group. In other words, a group is declared as satisfying when all the group parameters are true (AND model). All the groups are evaluated on the same lines. Then the node under observation is declared as untrusted only when the disjunction of all the groups' outcomes is true (OR model). Table I shows the comparison of AND and OR Models.

TABLE I. AND-OR MODEL COMPARISON.

Model	Risk	Attestation Overhead	False +ve	False -ve
AND	High	Low	No	Yes
OR	Low	High	Yes	No

Let the probability of a node declared as untrustworthy when all the parameters are considered individually be p_1, and the probability of the same node declared as untrustworthy when some (potentially distinct subset or group) of the parameters are considered conjunctively is p_2. It can be intuitively derived that $p_2 < p_1$. Based on this, the following conclusion is drawn:

Less number of nodes will be identified as untrustworthy in Parameter Grouping Model than the OR Model. It means that PG model results in less overhead in software attestation.

Let q_1 be the probability of a node declared as untrustworthy when all the parameters are considered as conjunctively, and q_2 be the probability of the same node declared as untrustworthy when disjunctions of groups of parameters are considered. It can be intuitively derived that $q_2 > q_1$. Based on this, the following conclusion is drawn:

Relative to AND Model, more number of nodes will be identified as untrustworthy in Parameter Grouping Model. It implies that more number of nodes are declared as untrustworthy when any one group of parameters is valid. It means that false negative rate (attack risk) is reduced compared to AND Model. It is to be observed that AND and OR models helps each other to mitigate the disadvantage of the other.

We can deploy AND-OR model and Parameter Grouping in different types of applications of WSNs, namely, military surveillance, weather monitoring etc.,

We discuss parameter grouping in detail in the next section.

IV. PARAMETER GROUPING

The motivation for parameter grouping is to overcome the demerits of AND, as well as OR Models. Parameter grouping is done based on their inter-relationship, for example, packet sending rate and depletion of node energy are inter-related as high packet sending rate results in high Depletion of Node Energy (DNE). The parameters mentioned earlier are categorized into three groups, namely, G1, G2, and G3, where G1={Packet Sending Rate, Depletion of Node Energy }, G2={Node Location, False Information}, G3={Non-Availability}. Mathematically, the concept of parameter grouping is explained below:

$$Node_iSusp = \begin{cases} (PSR_i \wedge DNE_i) \vee (NL_i \wedge FI_i) \vee (NAN_i) \\ or \\ (G1_i \vee G2_i \vee G3_i) \end{cases} \quad (3)$$

where G1=($PSR_i \wedge DNE_i$), G2=($NL_i \wedge FI_i$), G3=(NAN_i), and i^{th} node is suspected.

A. Group1 (G1)

The parameters, namely, PSR and DNE are made as one group, say G1. It means that the conjunction of the two parameters becomes true only when both the parameters are satisfied. If at least one parameter is not satisfied, the group outcome becomes negative irrespective of the other parameter's validity. Here G1= (PSR $\wedge$ DNE).

Packet Sending Rate: It is assumed that each sensor node sends a packet to ZH in every interval. The packets sent by all the members of the zone are maintained in a table. If any one node sends more number of packets abnormally, that is noticed by ZH. Then it determines that node's PSR value is True. Mathematically, PSR value of a i^{th} node at time interval k is

$$PSR(Node_i, TimeInterval_k) = \begin{cases} True, p_i > Th \\ False, else \end{cases} \quad (4)$$

where p_i is a number of packets received by i^{th}.

Depletion of Node Energy: As every node sends only one packet regularly to ZH, its battery energy depletes (consumes) uniformly. If some node's energy depletes quite fast (might be due to high packet sending rate), it becomes abnormal. The ZH notices this abnormality and suspects that node is compromised. Our assumption is that if any node's energy is decreasing more than threshold value in each interval, then that node's DNE value is considered as True.

$$DNE(Node_i, TI_k) = \begin{cases} True, Pre_{en} - Cur_{en} > Th \\ False, else \end{cases} \quad (5)$$

where i is $node_{id}$, k is time interval, TI is $TimeInterval_k$, Pre_{en} is the node's energy in the previous interval and Cur_{en} is the node's energy in the current interval.

After finding out the values of PSR and DNE, the G1's validity and then equation 3 are to be evaluated.

B. Group2 (G2)

The parameters, node location and false information are considered as one group. The reason for combining the two parameters is when an attacker physically captures a node, makes it compromised, and replaces it back at different location usually. As it is compromised, the node is likely to send false information to ZH. In other words, a node is suspected only when its location is changed and the information communicated by it to ZH is incorrect/unusual. G2= (NL $\wedge$ FI). If at least one parameter is false, then G2 is false.

Node Location: As we are dealling with static sensor network, nodes' location remains unchanged usually. The ZH maintains the locations of all the nodes, and suspects those nodes which change their locations unusually.

$$NL(Node_i, TI_k) = \begin{cases} False, if(Org_{loc} == Cur_{loc}) \\ True, else \end{cases} \quad (6)$$

where i is $Node_{id}$, k is time interval, Org_{loc} is the node's orginal location, and Cur_{loc} is the node's current location.

False Information: A sensor node is expected to communicate to ZH in a predefined format with an expected size, which is coherent with all other nodes reports. Contrary to this, if ZH notices incorrect and/or unusual information (in terms of size and format), that node is suspected.

After finding out the values of NL and FI, the G2's validity and then equation 3 is to be evaluated.

C. Group3 (G3)

This group has the only one parameter, NAN. Any new parameter which is coherent with this will be added to the group. If a particular node is unavailabe for communication because of physical capturing and compromisation activity, it is observed by ZH as unusual or abnormal. Then that node is declared as suspicous.

Algorithm 1 NAN algorithm

```
Gather all NodeID's & timestamp
Search all the nodes exist or not
if missing time > th then
    G3 or NAN=True
else
    G3 or NAN=False
end if
```

By substituting the values of G1, G2, and G3 the equation 3 is evaluated. If at least one of the Group $(G1, G2, G3)$ is true, then the corresponding is node considered as untrusted. The ZH informs to base station, when the untrusted nodes are identified.

V. Simulation

An extensive simulation study was carried out using NS2 simulator (NS2.35) on Ubuntu platform. As mentioned in Section III the network model consists of four zones with a total of 25 nodes including four zone heads and one base station, as shown in Figure 3. The routing and transport protocols used in our simulation are DSDV (Destination Sequenced Distance Vector) and UDP (User Datagram Protocol), respectively. The energy model is also included to know the residual battery energy of a node whenever required. Simulation was carried out based on the proposed concept of Parameter Grouping, and results are analyzed.

A. Experimental Analysis

All the parameters considered in simulation and their values/ranges are specified in Table II. The simulation was carried out by changing the number of nodes as 25, 30, 40, and 50. The atomic unit of time for our simulation is 1 sec. Behaviour

 ISBN: 978-1-61208-493-0

of sensor nodes is analyzed based on the statistics gathered during the simulation.

TABLE II. SIMULATION PARAMETERS.

Parameter	Value
Simulation Time	20 Seconds
Area	100 × 100
Time Intervals	1 Second
Traffic Type	UDP
Routing protocol	DSDV
Energy Model	Yes
No.of Nodes	25,30,40,50

Node Trust, The first experiment was carried out by setting the number of nodes as 25 and statistics, namely, event time, nodeID, energy, location (both x and y), the number of packets transmitted are collected and tabulated in Table III. It is to be observed that all the parameters are taking values as expected. No parameter is found with abnormal value. Hence, it is concluded that all the nodes in four zones are trustworthy. In other words, no node is found that is untrustworthy. This is also supported by the report of our NCD reporting system (based on NS2 simulation).

TABLE III. NODE TRUST.

Sender					
Time	NodeID	Energy	X-value	Y-value	#packets
.	.	.	.	.	.
11.7036	13	10.00	12.0000	20.0000	1
11.1895	5	9.99	8.0000	24.0000	1
11.0475	7	10.00	95.0000	72.0000	1
11.7449	10	10.00	60.0000	14.0000	1
11.0791	9	10.00	16.0000	25.0000	1
11.1886	8	10.00	28.0000	94.0000	1
11.7540	14	10.00	65.0000	18.0000	1
11.1138	15	10.00	85.0000	90.0000	1
11.8824	11	10.00	80.0000	82.0000	1
11.3390	6	10.00	71.0000	12.0000	1
11.1443	16	10.00	33.0000	90.0000	1
11.3334	12	10.00	35.0000	90.0000	1

The second simulation was carried out assuming that the attack took place. It means that some nodes are physically captured, compromised and re-located back at different locations. By observing the values of the identified parameters in Table IV, abnormality can be noted.

With respect to node 8 entry in Table IV, G1 parameters: PSR and DNE are true; and hence, the G1 also becomes true. Similarly G2's truth value (based on location and false information , as well as, G3's truth value becomes true. Hence 5, 8, and 10 are untrusted.

If we assume that a WSN is deployed for military surveillance application, an attacker can make the captured node to always report false (or misleading) information. For example, a particular compromised node reporting vehicle motion all the time.

Node Compromise Detection and Revocation: where Ntype is Node type, SN is suspicious node, CD is compromised node, ED is energy depletion and NAN is Non-Availability of Node.

TABLE IV. NODE UNTRUSTED.

Sender					
Time	NodeID	Energy	X-value	Y-value	#packets
.	.	.	.	.	.
11.1383	16	10.00	33.0000	90.0000	1
11.2395	13	10.00	12.0000	20.0000	1
11.9203	14	9.99	65.0000	18.0000	1
11.7560	5	9.99	12.7100	31.4100	1
11.3239	8	9.97	28.0000	94.0000	201
11.7636	9	9.99	16.0000	25.0000	1
11.2148	15	10.00	85.0000	90.0000	1
11.8340	12	9.99	35.0000	90.0000	1
11.3681	7	10.00	95.0000	72.0000	1
11.4029	10	9.97	60.0000	14.0000	201

TABLE V. COMPROMISED NODES.

NodeID	Energy	X	Y	packets	Ntype	CD	Comments
8	-	28.00	94.00	201	SN	yes	packets>Th
8	0.03	28.00	94.00	-	SN	yes	ED>Th
10	-	60.00	14.00	201	SN	yes	packets>Th
10	0.03	60.00	14.00	-	SN	yes	ED>Th
5	-	13.26	32.26	1	SN	yes	false location
6	-	-	-	-	SN	yes	NAN
11	-	-	-	-	SN	yes	NAN

As mentioned in Section I, the node is declared as compromised (NCD) if a node is untrustworthy and if the code is altered. It is to be noted that whether the code is altered or not is known through software attestation process; see Table V for the NCD report of the proposed and developed system. The compromised nodes are 5, 6, 8, 10, and 11 as per the report of the developed system. The MD5 (Message Digest) algorithm [16][17] is used for attestation. Compromised nodes can be revoked in two ways, first; one re-configure code of the compromised nodes, and secondly remove from the sensor network and replace with new nodes.

B. Performance Analysis

Let 'k' be the number of zones, each having 'm' number of nodes as its members on an average. If we assume that at least one zone is untrustworthy, then it is necessary for the BS to communicate the code for software attestation to each and every node of that zone (as per ZoneTrust concept). Hence, the communication cost is of the order n=$k \times m$ (total number of the nodes). Hence, the communication cost of ZoneTrust is O(n).

If we use the Parameter Grouping concept, the complexity decreases to O(k), where $k << n$. It is due to the need of BS to communicate only with identified untrusted nodes.

As explained above, the computation complexity (to run MD5 algorithm) of ZoneTrust is O(n), whereas that of the proposed PG concept is O(k) where $k << n$.

We apply the standard metrics of performance for detection systems [15].

- **False Positives**: It means that some benign nodes are reported as compromised. The PG model eliminates false positive reports. Systems with a low percentage of false positives are accurate.

 ISBN: 978-1-61208-493-0

- **False Negatives:** It implies that compromised nodes are reported as benign nodes. The PG model avoids false neagtive also.

Figures 4, 5, 6, and 7 show the performance between Parameter Grouping and ZoneTrust concepts in terms of Detection time, Number of Nodes to be Software Attested, communication overhead and computation overhead, respectively.

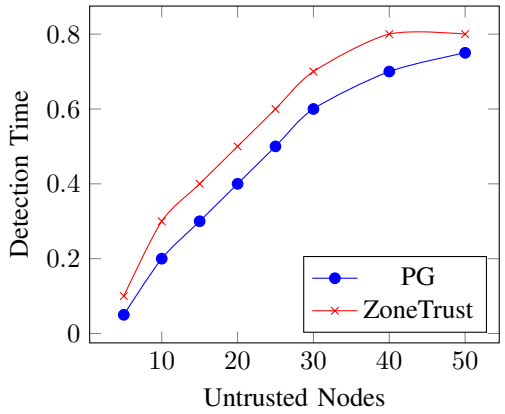

Figure 4. #Untrusted Nodes Vs Detection Time.

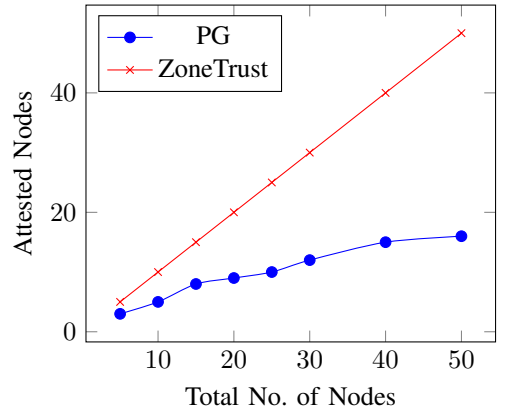

Figure 5. #Untrusted Nodes Vs #Nodes to be Attested.

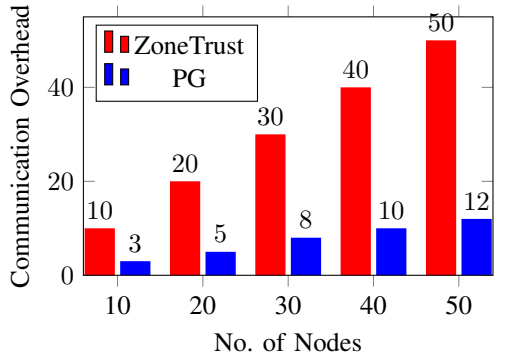

Figure 6. Communication Overhead between ZT and PG.

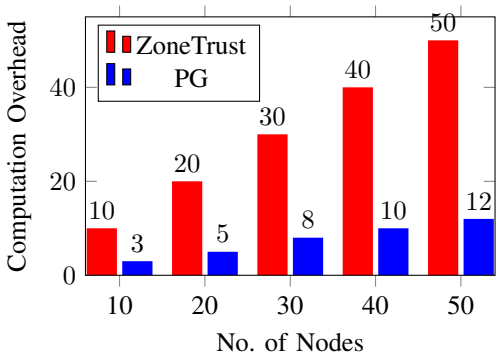

Figure 7. Computation Overhead between ZT and PG.

VI. Conclusion and Future Work

In this paper, Parameter Grouping concept for NCD in WSN was proposed, simulated and analyzed. The analysis, as well as simulation results prove that the computation and communication cost of the proposed method is O(k), whereas that of ZoneTrust method is O(n) where K is the number of zones and n is the total number of sensor nodes in WSN and $k << n$.

The proposed solution is to carry out further experimentation of Parameter Grouping concept by considering various node compromise models based on probability theory. The models are basic uniform, basic gradient, intelligent uniform, and intelligent gradient. This is to increase security and decrease the overhead of the system.

References

[1] Jun-Won Ho, Matthew Wright, and Sajal K. Das, "ZoneTrust: Fast Zone-Based Node Compromise Detection and Revocation in Wireless Sensor Networks Using Sequential Hypothesis Testing," IEEE Transactions on Dependable and Secure Computing, July/August 2012, vol. 9, no. 4, pp. 494-511.

[2] T. Abuhmed, N. Nyamaa, and D. Nyang, "Software-Based Remote Code Attestation in Wireless Sensor Network," Proc. of IEEE GLOBECOM, December. 2009.

[3] T. Park and K. G. Shin, "Soft Tamper-Proofing via Program Integrity Verification in Wireless Sensor Networks," IEEE Trans.Mobile Computing, May/June 2005, vol. 4, no. 3, pp. 297-309.

[4] A. Seshadri, A. Perrig, L. van Doorn, and P. Khosla, "SWATT:SoftWare-Based Attestation for Embedded Devices," Proc. IEEE Symp. Security and Privacy (S & P), May 2004.

[5] Mary Mathews, Min Song, Sachin Shetty, and Rick McKenzie, "Detecting Compromised Nodes in Wireless Sensor Networks," Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, August 2007, vol .1, pp. 273-278.

[6] F. Li and J. Wu, "Mobility Reduces Uncertainty in MANET," Proc. IEEE INFOCOM, May 2007.

[7] Perrig A, et al., "SPINS: security protocols for sensor networks," Presented at the 17th ACM international Conference on Mobile Computing and Networks (MobiCOM), 2001.

[8] Daniele Raffo, "Security Schemes for the OLSR Protocol for Ad Hoc Networks," 2005

[9] Miao Xie, Song Han, Biming Tian, and Sazia Parvin, "Anomaly detection in wireless sensor networks: A survey," Journal of Network and Computer Applications, July 2011, vol. 34, no. 4, pp. 1302–1325.

[10] Tao Li, Min Song, and Mansoor Alam, "Compromised Sensor Nodes Detection: A Quantitative Approach," The 28th An IEEE International Conference on Distributed Computing Systems Workshops, 2008.

[11] Vinayaka S.N, and M Dakshayini, "COMPRO-MOTO: An efficient approach for identifying compromised nodes in wireless sensor networks," International Journal of Computers and Technology, May 22, 2014, vol. 13, no. 7.

 ISBN: 978-1-61208-493-0

[12] B. Li, and R. Doss, "Fast Recovery from Node Compromise in Wireless Sensor Networks," An IEEE Third International Conference on New Technologies, Mobility and Security (NTMS), 2009
[13] Available online: http://www.wsn-security.info/Security_Map.htm (accessed on 1.05.2016).
[14] Manyam Thaile, and O.B.V Ramanaiah, "Node Compromise Detection Based on NodeTrust in Wireless Sensor Networks," An IEEE International Conference on Computer Communication and Informatics (ICCCI), Jan. 07 – 09, 2016, pp. 193-197, Coimbatore, INDIA
[15] Yi-Tao Wang, and Rajive Bagrodia, "ComeSen: A Detection for Identifying Compromised Nodes in Wireless Sensor Networks," SECURWARE 2012: The Sixth International Conference on Emerging Information, Systems and Technologies, pp. 148-156, 2012.
[16] S. Bruce, "Applied cryptography: protocols, algorithms and source code in C," John Wiley and Sons, Canada, 1996.
[17] S. Goldwasser, S. Micali, and R. Rivest, "A digital signature scheme secure against adaptive chosen-message attacks," J. Comput., vol. 17, no. 2, pp. 281-308, 1988.

 ISBN: 978-1-61208-493-0