Hierarchical Trust-based Black-Hole Detection in WSN-based Smart Grid Monitoring

Safa Otoum, Burak Kantarci, and Hussein T. Mouftah

School of Electrical Engineering and Computer Science, University of Ottawa,
Ottawa, ON, Canada

Abstract —Wireless Sensor Networks (WSNs) have been widely adopted to monitor various ambient conditions including critical infrastructures. Since power grid is considered as a critical infrastructure, and the smart grid has appeared as a viable technology to introduce more reliability, efficiency, controllability, and safety to the traditional power grid, WSNs have been envisioned as potential tools to monitor the smart grid. The motivation behind smart grid monitoring is to improve its emergency preparedness and resilience. Despite their effectiveness in monitoring critical infrastructures, WSNs also introduce various security vulnerabilities due to their open nature and unreliable wireless links. In this paper, we focus on the, Black-Hole (B-H) attack. To cope with this, we propose a hierarchical trust-based WSN monitoring model for the smart grid equipment in order to detect the B-H attacks. Malicious nodes have been detected by testing the trade-off between trust and dropped packet ratios for each Cluster Head (CH). We select different thresholds for the Packets Dropped Ratio (PDR) in order to test the network behaviour with them. We set four different thresholds (20%, 30%, 40%, and 50%). Threshold of 50% has been shown to reach the system stability in early periods with the least number of re-clustering operations.

***Keywords* — Black-hole attack, data aggregation, hierarchical trust evaluation, smart grid monitoring, weighted clustering, wireless sensor networks.**

I. INTRODUCTION

Wireless Sensor Networks (WSNs) have been identified as a strong candidate to meet the major smart grid communication requirements, namely self-monitoring and configurability WSNs employ diverse types of sensors, i.e.: thermal, visual, radar, infrared and magnetic which help in increasing their ability to monitor a variety of conditions such as humidity, pressure, temperature, and noise levels [1][2].

Smart grid enables better utilization of various energy sources, such as wind and solar into the generation system [3]. It can also help in saving energy, increasing the network reliability, increasing the process efficiency, and reduce costs. The efficiency and reliability of this technology are important factors achieved by accomplishing secure and reliable data aggregation and transmission. It is vulnerable to various cyberattacks since it relies on the information technologies. Thus, any interference with the control unit would cause irreversible consequences either locally or nationwide. Furthermore, communication lines are vulnerable to jamming attacks that can interrupt the communication and play a vital role in manipulating the transmitted signals between the customers and distribution links. Lately, WSNs have been used in smart grids because of low cost, flexible, self and rapid deployment features and fault tolerance [4][5][6].

Some sensors are intended to monitor the energy usage or the quality of the power lines which are directly related to the smart grid. Integration of WSNs with smart grids introduced additional security threats to both domains. The security vulnerabilities of smart grids can be in the cyber domain such as attacks on the communication links or in the physical domain such as attacks on distribution or transmission lines. Black-Hole (B-H) attack is an example of the cyberattacks.

B-H is a routing layer attack and one of the emerging security threats in networks where the attackers apply loophole to spread malicious behaviour [1]. It occurs when a node blocks or drops the packets it receives instead of forwarding them towards the receiving node [7]. Thus, any data that traverses the black hole nodes is blocked which leads to performance degradation in network efficiency and excessive energy consumption.

In this paper, we aim to address the aforementioned challenges in order to advance the state of the art, and propose a B-H detection model in WSN-based smart grid applications, which can detect the B-H Cluster Heads (CHs) by finding out the trade-off between the packet dropped ratio and trust score which refers to the node evaluation based on its honesty, selfishness, energy, and intimacy factors. In addition, re-clustering operations are performed in order to elect legitimate CHs instead of the malicious ones.

Various thresholds (50%, 40%, 30% and 20%) for packet dropped ratios have been chosen in order to test the network behaviour for different values. By using various thresholds, re-clustering operations are varied in the starting periods. Starting period denotes the time interval where the trust scores are re-assessed for possible re-election of cluster heads in the network. Re-election of cluster heads is started on the basis of the trust score assessments. Varying the re-clustering operations in, the starting period, impacts the number of re-clustering operations. Our simulation results show that when the threshold is set to 50%, the system can stabilize earlier with less number of re-clustering operations.

The rest of the paper is organized as follows. In section II, we give a brief review of the related work. In section III, we formalize the proposed system model. Section IV presents the performance evaluation of the proposed model. Finally, in Section V, we conclude the paper and give future directions.

II. RELATED WORK

Addressing security vulnerabilities is the most crucial issue in WSN-based smart grid applications. Distributed evaluation of trust scores plays a vital role in distinguishing

978-1-4673-8999-0/17/$31.00 ©2017 IEEE

between normal and malicious devices [8]. Malicious devices can be attackers that threaten the security of the whole network. Replacing malicious devices help in achieving the security of the network. In [9], the researchers proposed an exponential trust-based mechanism in order to detect the black-hole attacks. In their proposed model, they introduce nodes with trust factors and a counter of the dropped packets which helps them in detecting the malicious nodes. The trust factors of the nodes are calculated by the exponential formula $100x^{ni}$where n is the counter value.

In [10], the authors propose an algorithm to overcome the black-hole and grey-hole attacks. The grey-hole attack has the same behaviour as the black-hole; however, it does not drop whole packets as black-hole but drops a sub-stream of an incoming packet stream instead. The algorithm is based on dividing the data into smaller data blocks to discover the malicious nodes. The neighbouring nodes collaborate in the transmission of the data blocks from the source towards the destination. The acknowledgements by the destinations help in the detection of malicious nodes.

The authors in [11] propose a hierarchical secure routing protocol against B-H attacks by using the symmetric key cryptography to find out the secure route. The authors divided the proposed network into a number of groups organized as a tree topology, each group leader acts as a root of the tree. The black-hole attack was detected by using the randomized data acknowledgement scheme.

TABLE 1. NOTATIONS USED IN THE SYSTEM MODEL

Notation	Description
dn	Degree of node *n*
$\mathit{\Delta n}$	Nodes degree difference
$SumSTm$	Sum of received signal strength
Mn	Node *n* mobility
Tm	Time for being a *CH*
Wn	Combined nodes weights
T_{agg}	Aggregator trust value
T_{agg}, n	Trust evaluation between the aggregator and node *n*
T_n	Node *n* trust value
T_{nm} (t)	Trust evaluation between nodes *n* and *m* at time-t
$T_{nm}^{inti}(t)$	Node intimacy evaluation
$T_{nm}^{hons}(t)$	Node honesty evaluation
$T_{nm}^{ener}(t)$	Node residual energy
$T_{nm}^{unslsh}(t)$	Node unselfishness level

In [12] the authors propose an efficient and trust based secure protocol to protect against single and cooperative B-H attack. In their proposed protocol, the trust metrics are used to find a node's honesty during a secure path formation. As a result, the proposed protocol achieves acceptable performance in secure routing and a certain level of robustness against both single and cooperative black-hole attacks.

III. HIERARCHICAL TRUST-BASED BLACK-HOLE DETECTION

We consider a clustered network that consists of a central server and *N* clusters each consisting of *M* sensor nodes. In each cluster, the cluster head (CH) assumes the responsibility of data aggregation. Each sensor node forwards its sensed data to its corresponding CH which aggregates the data and forwards it to the central sink, which can be a centralized server. Before we proceed with the details of the model, in Table I, we present the notation that is used in the presentation of the system model, and the proposed scheme.

A. *Cluster Head Selection*

The selection of the CH has been done by using the weighted cluster head selection algorithm [13], in which the CH is selected on the basis of a comparison of the *weight* of each node with the other nodes inside the cluster. In the weighted cluster head selection method, each node is assigned a weight which is a function of its node degree, received signal strength and mobility. The weighted cluster head selection method passes through the following consecutive steps: Finding the node degree d_n of each node *n*, computing the degree of difference $\mathit{\Delta n}$, computing the sum of received signal strength *SumSTn*, computing the node's mobility M_n, computing the cumulative time Tm which denotes the time elapsed since the node *m* has represented as a CH and finally calculating the combined node weights. The combined node weight equation is represented in (1) below [13]:

$$Wn = w_1 \mathit{\Delta n} + w_2 \left| \frac{1}{SumSTn} \right| + w_3 Mn + \; w_4 Tn \qquad (1)$$

In the equation $\mathit{\Delta n} = \left| \, d_n \text{ - } \delta \right|$ and $\left| 1/SumSTm \right|$ is the normalized received signal strength sum. Every node calculates its own weight and broadcasts it with its ID then it compares its own weight with its neighbours' weights. The node with the minimum weight is selected as the CH.

B. *Data Aggregation*

Data aggregation is an essential process in networking which helps in excluding the resulted redundancy of sensing data, saving the nodes energy, overcoming the communication overhead issues, and elimination of outlier sensor readings [14].

In our proposed network, each CH acts as the aggregator for its corresponding cluster where the data aggregation has been done based on each node's trust values. Each CH aggregates the data from the other nodes in its cluster and sends the aggregated data to the centralized sink. The data aggregation method in [14] has been adopted by our proposed system.

The aggregation function in (2) below [14] has been used in our proposed model in order to calculate the trust of CHs which are represented as the aggregators here T_{agg} is the aggregator trust value, T_n is the node n trust value and T_{agg}, n is the trust evaluation between the aggregator and node n.

$$T_{agg} = (\sum_{n=1}^{k} (T_n + 1) * T_{agg}, n \,) \,/(\, \textstyle\sum_{n=1}^{k} (T_n + 1) \,) \qquad (2)$$

C. *Hierarchical trust evaluation*

Our proposed method adopts the peer-to-peer (P2P) hierarchical trust evaluation process in [15] in order to evaluate the trust between the sensor nodes that are installed on the critical smart grid equipment, such as the smart meters (SMs) and the phasor measurements units (PMUs). We have also used the P2P hierarchical trust evaluation to distinguish the legitimate nodes from illegitimate nodes and to build a secure data aggregation scheme in the CHs which can assess the trustworthiness of sensor nodes in their clusters.

The hierarchical trust evaluation method considers both the Quality of Service (QoS) and the social factors. The QoS factors are the energy and the unselfishness. While the intimacy and the honesty fall under social factors. The Hierarchical trust evaluation method in [15] is described in the following lines:

T_{nm} (t) is a real number in [0,1] range and it represents the trust evaluation between node-*n* and node-*m* at time-*t*.

$$T_a = F_1 T_{nm}^{inti}(t) \tag{3}$$

$$T_b = F_2 T_{nm}^{hons}(t) \tag{4}$$

$$T_c = F_3 T_{nm}^{ener}(t) \tag{5}$$

$$T_d = F_4 T_{nm}^{unslsh}(t) \tag{6}$$

In the equation set, F_i represents the weights associated with the components. The social factors and the QoS factors are formulated in (7) and (8), respectively.

$$T_{social} = T_a + T_b \tag{7}$$

$$T_{QoS} = T_c + T_d \tag{8}$$

The trust evaluation is computed by the equations below in (9) and (10):

$$T_{nm} = T_a + T_b + T_c + T_d \tag{9}$$

$$\begin{aligned} T_{nm} = F_1 * \ T_{nm}^{inti}(t) + F_2 * T_{nm}^{hons}(t) + \ F_3 \\ * T_{nm}^{ener}(t) + \ F_4 * T_{nm}^{unslsh}(t) \end{aligned} \tag{10}$$

In the equations, $T_{nm}^{inti}(t)$ represents the intimacy which refers to the level of interaction between nodes n and m.$T_{nm}^{hons}(t)$: stands for the node honesty which is increased when a node performs its proposed functions successfully. Packet drops or detected attacks by a node leads to marking that node as dishonest. $T_{nm}^{ener}(t)$ represents the level of residual energy of the node, and $T_{nm}^{unslsh}(t)$ denotes the unselfishness level of the node. A typical behavior of a selfish node is stopping sensing tasks and dropping its received packets to save energy.

The overall system model is illustrated in Figure 1. The system consists of *N* clusters. The CHs are the forwarding nodes. The aggregated data is moved to the centralized sink which is connected with the cloud in order to save the data. The proposed system aims to achieve a secure and private data environment by maintaining B-H-proof environment.

The Dynamic Source Routing (DSR) protocol has been employed in the routing layer in the proposed model in order to achieve the required efficiency because of its advantages of minimizing the overhead. Each CH checks for a B-H attack before aggregating the incoming data from the nodes inside its cluster.

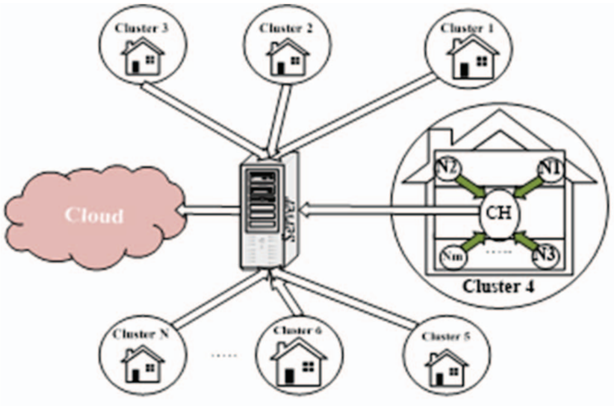

Figure 1. Overall system model

Our work focuses on detecting the B-H attack in order to achieve secure communication and secure data aggregation. In order to achieve a successful aggregation operation, we have to ensure that the CHs are resilient against attacks. Each CH keeps track of its dropped packets in order to avoid any B-H occurrences. Thus, the ratio of dropped packets (PDR) should be less than a pre-defined threshold. In case of the PDR being larger than the threshold, a re-clustering operation should be considered.

Our strategy is presented in the flowchart in Figure 2. Initially, each node is assumed to maintain 100% trust score. Second, weighted clustering operation is implemented in order to elect a CH for each cluster which is the aggregator node. Due to the aggregator importance, the trust scores of the CHs and their corresponding sensor nodes are also assessed periodically. In order to keep track of CHs effectiveness, PDR-based trust score assessment is called: If the PDR of a CH exceeds a pre-defined threshold, we consider the corresponding CH as a B-H node and a re-clustering operation is triggered to elect a new CH for this cluster.

TABLE II. SIMULATION SETTINGS

Simulation parameter	Value
Number of nodes	20
Number of clusters	4
Routing protocol	DSR
Simulation time	120s
Packet size	250 bytes
Communication range	100m
Trust range	[0,1]
Thresholds	20%, 30%, 40% and 50%
Operational area	100m x 100m

The complexity analysis of our hierarchical model is $O(mn)$, where m and n refer to the number of clusters and nodes inside each cluster respectively.

$$O(mn) = O(mm) = O(m\text{^}2) \tag{11}$$

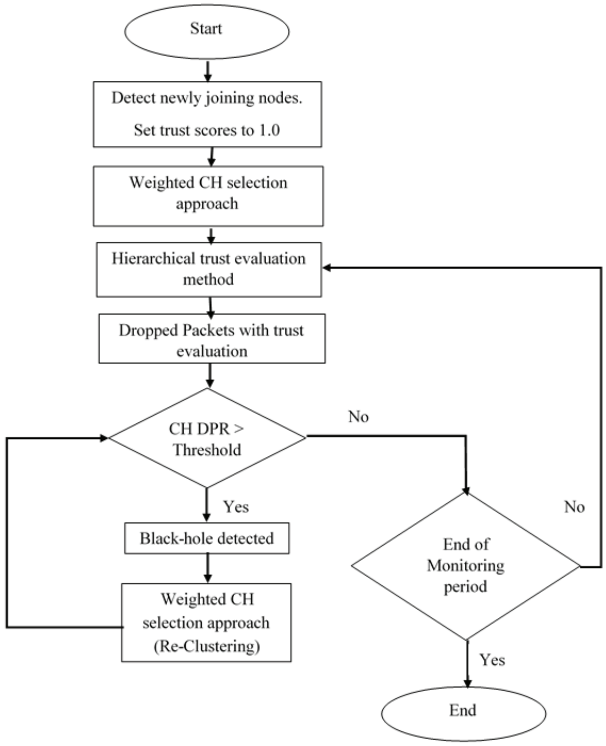
Start
Detect newly joining nodes.
Set trust scores to 1.0
Weighted CH selection approach
Hierarchical trust evaluation method
Dropped Packets with trust evaluation
CH DPR > Threshold
No
Yes
Black-hole detected
Weighted CH selection approach (Re-Clustering)
End of Monitoring period
No
Yes
End

Figure 2. Black-hole (B-H) detection flowchart

IV. Performance Evaluation

The proposed evaluation is represented through graphs. The simulator used in the implementation of our proposed system is the NS-3 simulator, which is a discrete-event network simulator licensed under the GNU GPLv2. We have considered a network of 20 sensor nodes with 4 clusters spread out in a 100m x 100m area. Initially all sensors have a trust ratio of 100%. The trust ratios of the nodes decrease continuously with the network functions. The simulation settings along with the assumptions are summarized in Table II.

In order to test our proposed system model behaviour, we have run tests by setting the PDR threshold to the following values: 50%, 40%, 30% and 20%. Figures 3.(a)/(c)/(e)/(g) represent the pre-clustering phase values of the PDR with respect to varying trust score of each CH under the four thresholds. The post-clustering phase denotes the situation after a number of re-clustering attempts where each CH PDR is enforced to be under the defined thresholds.

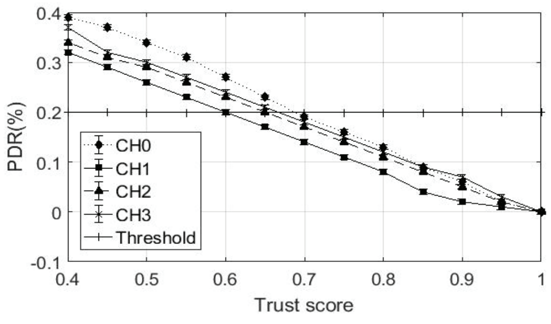

Figure 3.a. Pre-clustering phase for threshold of 20%.

We discuss the results based on each threshold value in the subsections bellow. In addition, the tables from Table III to Table VII represent the number of re-clustering operations for each CH with threshold values. The numerical results in the tables also represent the trust scores at which the re-clustering operations have started. The NRN notations refer to "No Re-clustering operations Needed" (NRN).

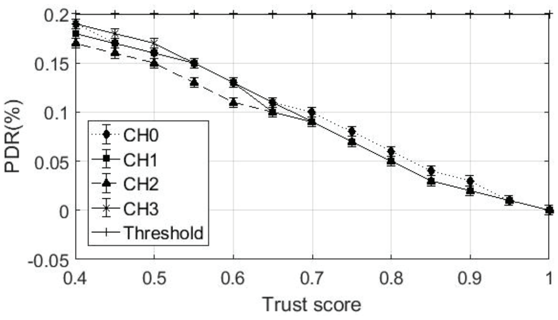

Figure 3.b. Post-clustering phase for threshold of 20%.

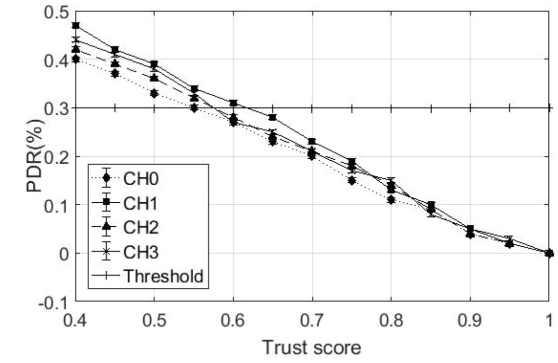

Figure 3.c. Pre-clustering phase for threshold of 30%.

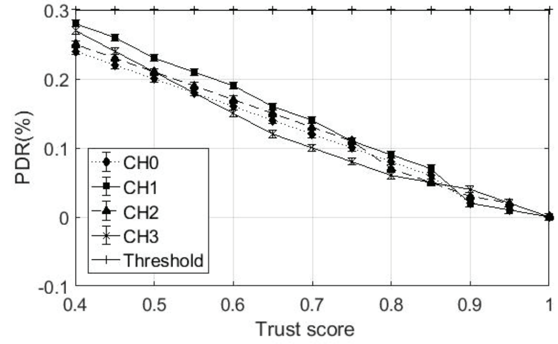

Figure 3.d. Post-clustering phase for threshold of 30%.

A. Threshold of 50%

From Figure 3(g), CH_3 has dropped packet ratio (PDR) larger than the chosen threshold (Threshold=50%). Accordingly, we have applied the re-clustering operation in order to elect another CH. The cluster's formation after two re-clustering operations is illustrated in Figure 3(h) where the PDR of all CHs stabilize under the 50%. Choosing a threshold of 50% needed two re-clustering operations to achieve a B-H free environment.

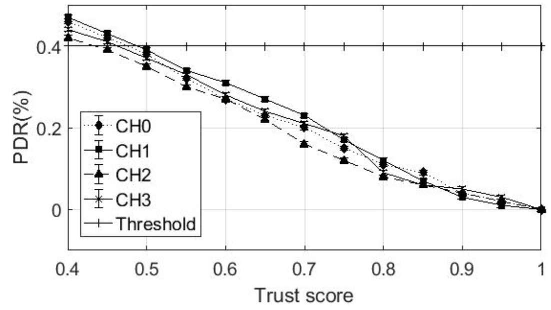

Figure 3.e. Pre-clustering phase for threshold of 40%.

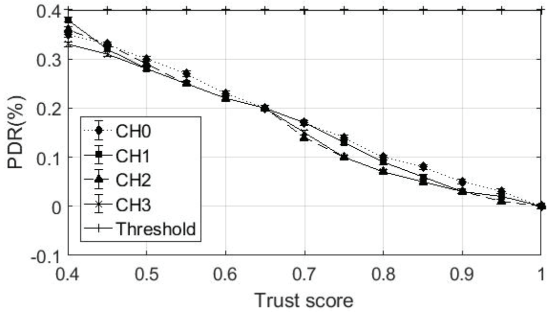

Figure 3.f. Post-clustering phase for threshold of 40%.

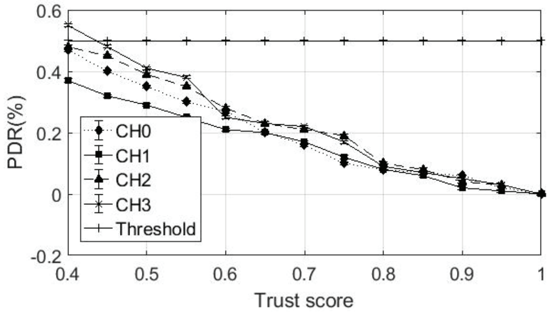

Figure 3.g. Pre-clustering phase for threshold of 50%.

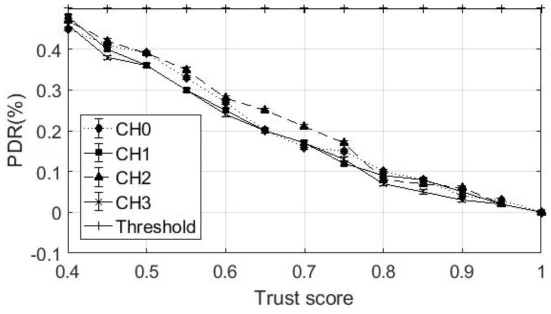

Figure 3.h. Post-clustering phase for threshold of 50%.

B. *Threshold of 40%*

The results under 40% threshold are presented in Figure 3 (e), (f). Three re-clustering operations have been taken place in order to achieve a B-H-proof environment. All CHs' PDRs have been exceeded the 40% threshold. As a result, all CHs have attempted the first re-clustering operation in order to elect four new CHs. After the first re-clustering, CH_0, CH_1 and CH_3 needed a second re-clustering operation due to their PDRs which exceeded the 40% threshold. Accordingly, for the second re-clustering, the PDRs of CH_0 and CH_3 have been reduced to less than 40% but CH_1 is still above the 40%. The need for third re-clustering attempt has arisen.

C. *Threshold of 30%*

The PDR with trust scores under 30% threshold is presented in Figure 3 (c) and (d). Choosing a threshold of 30% needed three re-clustering operations. As it shown in the figure, the re-clustering operations started in the early periods before the end of simulation time. From Tables III and IV, all CHs needed two re-clustering operations in order to elect new CHs. After two re-clustering attempts, --as also shown in Table V--, CH_1 and CH_3 needed a third re-clustering operation while the PDRs of CH_0 and CH_2 have reduced below 30%. As a result, for the third re-clustering operation, all CHs have been approved as secured CHs.

D. *Threshold of 20%*

In Tables III to VII, the threshold of 20% needs five re-clustering operations. The re-clustering operations started from early periods when the trust scores were around 70%. In the first four re-clustering operations, all CHs needed re-clustering. After the forth re-clustering operation, the PDR of CH_2 has been minimized to a value less than the 20% while CH_0, CH_1 and CH_3 needed a fifth re-clustering.

It is worthwhile noting that the aim of the proposed hierarchical trust evaluation-based black-hole detection model is to reduce the number of CH re-election in order to have a stable monitoring system for the critical infrastructure.

TABLE III. TRUST% CORRESPONDING TO FIRST RE-CLUSTERING OPERATION.

Threshold	Number of Re-clustering	CH0	CH1	CH2	CH3
20%	5	69%	60%	65%	66%
30%	3	55%	61%	57%	57%
40%	3	47%	49%	43%	46%
50%	2	NRN	NRN	NRN	44%

TABLE IV. TRUST% CORRESPONDING TO SECOND RE-CLUSTERING OPERATION.

Threshold	Number of Re-clustering	CH0	CH1	CH2	CH3
20%	5	56%	55%	60%	61%
30%	3	51%	56%	49%	52%
40%	3	44%	45%	NRN	41%
50%	2	NRN	41%	NRN	NRN

TABLE V. TRUST% CORRESPONDING TO THIRD RE-CLUSTERING OPERATION.

Threshold	Number of Re-clustering	CH0	CH1	CH2	CH3
20%	5	52%	55%	50%	47%
30%	3	NRN	47%	NRN	40%
40%	3	NRN	42%	NRN	NRN
50%	2	NRN	NRN	NRN	NRN

TABLE VI. TRUST% CORRESPONDING TO FORTH RE-CLUSTERING OPERATION.

Threshold	Number of Re-clustering	CH0	CH1	CH2	CH3
20%	5	45%	48%	45%	49%
30%	3	NRN	NRN	NRN	NRN
40%	3	NRN	NRN	NRN	NRN
50%	2	NRN	NRN	NRN	NRN

TABLE VII. TRUST% CORRESPONDING TO FIFTH RE-CLUSTERING OPERATION.

Threshold	Number of Re-clustering	CH0	CH1	CH2	CH3
20%	5	42%	40%	NRN	42%
30%	3	NRN	NRN	NRN	NRN
40%	3	NRN	NRN	NRN	NRN
50%	2	NRN	NRN	NRN	NRN

V. CONCLUSION

Bringing the use of sensors with smart grid networks introduces new challenges despite its advantages of achieving the promising efficiency and low costs. One of the most important issues is addressing the security issues and minimizing the cyber-physical security vulnerabilities. In this paper, we have proposed a Black Hole (B-H) detection system. According to the proposed B-H detection model, once B-H Cluster Heads (CHs) are detected, CH re-election procedures are triggered in order to achieve a B-H free environment which helps in forwarding the transmitted information securely and with minimum risk of information loss. To this end, we have adopted a hierarchical trust score evaluation method which is run for the CHs on the basis of a primary B-H indicator, namely the packet drop ratio (PDR) at the CH. We have studied the impact of various thresholds (50%, 40%, 30% and 20%) in order to test the system model behaviour. A PR threshold of 50% has been shown to reach the system stability in early periods with the least number of re-clustering operations. As one of the key performance factors in the WSNs is the network stability, we aim at minimum number of disruptions at the clusters. Our simulation results have shown that reducing the threshold ratio increases the number of re-clustering operations whereas in some cases all CHs can be considered as B-H nodes (in case of 20%). Although number of re-clustering attempts is intuitively an expected phenomenon by intuition, it is worthwhile mentioning that, while reducing the number of re-clustering attempts, we also ensure a B-H-free monitoring environment.

Besides the B-H detection issue, we are currently working on further detecting and mitigating all possible attacks that may interfere with the WSN-based smart grid network fields. Furthermore, we are currently implementing a hybrid intrusion detection system for the detection of internal and external intruders.

REFERENCES

[1] R. Kaur and P. Singh, “Review of black hole and grey hole attack”, The International Journal of Multimedia & Its Appli cations (IJMA), Vol.6, No.6, December 2014.

[2] S. Otoum, M. Ahmed and H. T. Mouftah, “Sensor Medium Access Control (SMAC)-based Epilepsy Patients Monitoring System”, Proceeding of the IEEE 28th Canadian Conference on Electrical and Computer Engineering Halifax, Canada, May 3-6, 2015.

[3] DOE, U.S., "Communications requirements of Smart Grid technologies", U.S.Department. Energy,Washington,DC, USA , 2010, pp. 1–69.

[4] V.C. Gungor, D. Sahin, T. Kocak, S. Ergut, C. Buccella, C. Ceca-ti and G.P. Hancke, ”Smart Grid technologies: communication technologies and standards”, In IEEE Transactions on Industrial Informatics, 2011, November, No. 4, p.529-539.

[5] V.C. Gungor, B. Lu and G. P. Hancke, “Opportunities and challenges of wireless sensor networks in Smart Grid”, In: IEEE Transactions on Industrial Electronics, 2010, October, No. 10, p. 3557-3564.

[6] H. Idoudi and M. Saed, “Security Considerations in WSN-Based Smart Grids”, International Conference on Security and Management (SAM’14), Las Vegas, USA, 2014.

[7] B. R. Baviskar and V. N. Patil, “Black hole Attacks Prevention in Wireless Sensor Network by Multiple Base Station Using of Efficient Data Encryption Algorithms”, International Journal of Advent Research in Computer & Electronics, Vol.1, No.2, April 2014, E-ISSN: 2348-5523.

[8] M. Pouryazdan, B. Kantarci, T. Soyata and H. Song, "Anchor-Assisted and Vote-based Trustworthiness Assurance in Smart City Crowdsensing" IEEE Access, vol. 4, pp. 529-541, Mar. 2016.

[9] S. Banerjee,“Detection/Removal of Cooperative Black and Gray Hole in Mobile Ad-Hoc Network”, WCECS 2008, San Francisco, USA, October 22-24, 2008.

[10] J. Yin and S. K. Madria, “A Hierarchical Secure Routing Protocol against Blackhole Attacks in Sensor Networks”, IEEE International Conference on Sensor Networks, 2006.

[11] G. R. Pathak, S. H. Patil and J. S. Tryambake, “Efficient and trust based black hole attack detection and prevention in WSN”, International Journal of Computer Science and Business Informatics, Vol.14, No.2, pp. 93–103.

[12] N. V. Babu, S. B. Boregowda, C. Puttamadappa and S. S. Davanakatti, " An optimized weight based clustering algorithm in heterogeneous wireless sensor networks", Computer Science & Information Technology (CS & IT 08), pp. 185–195, 2012.

[13] C. Mainak, K. D. Sajal and T. Damla, "WCA: A Weighted Clustering Algorithm for Mobile Ad Hoc Networks," Cluster Computing 5, pp. 193-204, 2002.

[14] J. Hur,Y. Lee,S. Hong,and H. Yoon,“Trust-based secure aggregathion in wireless sensor networks,” in Proceedings of the 3rd International Conference on Computing, Communications and Control Technologies, vol.3, pp.1–6, 2005.

[15] F. Bao, I.-R. Chen, M. Chang, and J.-H. Cho, “Hierarchical Trust Management for Wireless Sensor Networks and its Applications to Trust-Based Routing and Intrusion Detection”, IEEE transactions on network and service management, vol. 9, no. 2, june 2012.