DOI: 10.21917/ijct.2018.0274

THE RESEARCH ON ENERGY EFFICIENT WATCHING METHOD USING CLUSTER HEADER IN WSN

Won Chol Jang, Jong Ae Choe and Du Ho Pak

College of Information Engineering, WonSan Jogunsil University of Technology, D.P.R. of Korea

Abstract

Many problems in WSN security are same as in the traditional network. However, some problems are different at all in computer network such as internet, because of characteristics of WSN self. Sensor nodes of WSN cannot use coding such as public key, complicated authorization and the firewall, because sensor nodes have limited energy and there are little hardware resources such as computation, memory and signal processing. So, recently, they have researched on secure routing and configuration of trust system and optimization of watching node alignment. In previous works, they referred the watching attack of WSN of which topology is routing, but they have not referred the watching attack of WSN of which topology is clustering. First, we configure trust system and propose the optimization of watching node's position and watching period in clustering WSN in this paper. Second we compare and analyze the proposed method and the method in routing WSN by mathematical modeling.

Keywords:

WSN, Routing, Security, Trust System

1. INTRODUCTION

Secure routing base on trust system has been attracted as the most powerful method recently. The trust system provides WSN security, as various sensor node analyzed change of routing and behavior, assesses each other. This system is one type of cooperation and filter algorithm of entities belonging to the identical group. All sensor nodes assess the trust of other sensor nodes through gathering of received data from other nodes. Most of trust systems depend on analyzation of inclusive network. The trust of sensor node is usually determined by portion of corresponding node contributed to data packet gathered by other node received data packet from the node in MANET (Mobile Ad hoc Network) and WSN. There are CONFID ANT [1], SORI [2] and CORE [3] and so on in the trust system used in MANET and WSN. However, there is some differences between MANET and WSN.

- First, WSN has limited resources unlike MANET.
- Second, the active condition and application field of WSN is different from MANET.
- Third, the communication model of MANET is a model between equal two nodes, but one of WSN is multi to one model between nodes of which positions of network are different.
- Fourth, routing control protocol, DSR of MANET is appropriate to WSN because of resource and efficiency.

From this, WSNode Rater, trust system of WSN was proposed in previous work [4]. WSNode Rater consists of three parts, watching system, estimation system and response system. The trust is estimated based on three parameters, the first information, the second information and reliable run time.

GESAR (Geographic, Energy and Security Aware Routing Protocol) proposed in [4] uses the defensive response. In GESAR, one of sensor nodes uses the trust of neighbor node for its route rejection. If the watching node is over trust section, it rejects the node's packet. In contrast, the watching node is in trust section, corresponding node can belong to the network. If the node is over trust section far away, the node is excluded in network forever.

Watching node optimization has been referred in many previous works [5], [6]. Energy efficient watching node optimization alignment has been referred in [7].

WSN is denoted by graph $G = (V,E)$, where $v_i \in V$ is a sensor node of WSN and $e_{i,j} \in E$ means that node i and j can communicate each other. The topology of WSN is routing, not clustering. If the distance between v_i and v_j is $d_{i,j}$ and the communication distance of v_i is r_i, $e_{i,j} \in E$, when $d_{i,j} \le r_i$, $d_{i,j} \le r_j$.

In this case, a set of neighbor nodes of node v_i, $B_i \le V$ is as follows.

$$B_i = \{v_j \,|\, e_{i,j} \in E\} = \{v_j \,|\, d_{i,j} \le r_i \ \&\ d_{i,j} \le r_j\}$$

The Fig.1 shows the example of WSN system model.

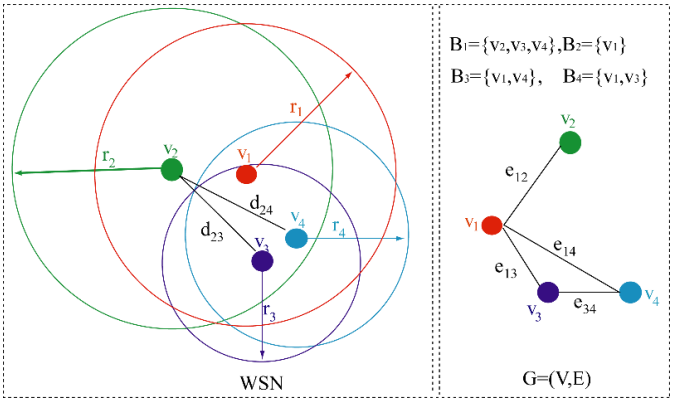

Fig.1. Example of WSN system model.

In order to estimate energy consumption model, they usually use the free propagation model that LEACH (Low-Energy Adaptive Clustering Hierarchy) used. Let E_{elec} be energy consumed on operate transceiver necessary to transmit and receive one bit and ε is propagation constant with unit J/bit/m^2.

Energy consumed on transmitting one bit is as follows.

$$\varepsilon_{ij}^{Tx} = E_{elec} + \varepsilon d_{ij}^2 \quad (1)$$

Energy consumed on receiving one bit from node v_i and v_j is as follows.

$$\varepsilon_{ij}^{Rx} = E_{elec} \quad (2)$$

If the watching task ω_{ij}^t requires L bit information for answer or response, energy that the watching node v_i consumes to do ω_{ij}^t is as follows.

$$\varepsilon_i(\omega_{ij}^t) = L\left(\varepsilon_{ij}^{Tx} + \varepsilon_{ij}^{Rx}\right) = 2 \cdot L \cdot E_{elec} + \varepsilon \cdot L \cdot d_{ij}^2 \quad (3)$$

Energy that the task node v_j consumes is as follows.

$$\varepsilon_j(\omega_{ij}^t) = \varepsilon_i(\omega_{ij}^t) \quad (4)$$

Given the attack node v_j, the probability that node v_i is attacked by node v_j is as follows.

$$\Pr\left\{v_i \in A \mid v_j \in A\right\} = \frac{1}{a \cdot d_{ij} + 1} \quad (5)$$

The trust of the node is determined by the expectation of the node during certain time. First they define I_{ij}^t, as the same event as expected by v_i during slot t. The trust is calculated as following.

$$T_{ij} = \frac{\sum_{t \in N, \omega_{ij}^t \in \varphi} I_{ij}^t}{\sum_{t \in N, \omega_{ij}^t \in \varphi} 1} \quad (6)$$

The accuracy and robustness of trust T_{ij} can be estimated by Kullback-Leibler distance. The total risk function is defined as follows.

$$F(d_{ij}) = 2L\varepsilon d_{ij}^2 + \frac{1}{\alpha d_{ij}} \quad (7)$$

The d_{ij} minimizing $F(d_{ij})$ is as follows.

$$d_{ij} = (4L\varepsilon\alpha)^{1/3} \quad (8)$$

$$\text{If } (4L\varepsilon\alpha)^{1/3} > r_j,\ d_{ij} = r_j.$$

In previous works, they referred the watching attack of WSN of which topology is routing, but they have not referred the watching attack of WSN of which topology is clustering.

First, we configure trust system and propose the optimization of watching node's position and watching period in clustering WSN in this paper. Second we compare and analyze the proposed method and the method in routing WSN by mathematical modeling.

2. PROPOSED METHOD

The watching node is a node watching if illegal data communication event occurs in the network. In general, the watching node agrees with following two conditions.

- First, the set of watching nodes can have to watch all nodes of network continuously.
- Second, the watching node performs watching during necessary time to watching and it is in sleeping mode to decrease energy consumption.

In order to satisfy the first condition, following number of watching nodes are needs at least.

$$N_{WATCH,\min} = \frac{N}{\overline{D}(G)} \quad (9)$$

where, $\overline{D}(G)$ is an average degree of network.

Also, in order to satisfy the second condition, the watching cycle is maximized under following condition.

$$T_{WATCH} \le T_{DATA} \quad (10)$$

$$T_{WATCH}(i) \le T_{DATA}(j)$$

That is, optimal watching cycle is satisfied following condition.

$$T_{WATCH}(i) = T_{DATA}(j) \quad (11)$$

We propose the method setting CH (Cluster Header) as watching node in scheduling WSN.

If CH is set as watching node, the first condition is almost satisfied. Because CH receives data from all nodes in cluster during its active time and send to high node or base station after gathering or processing.

If CH is set as watching node, the second condition is satisfied too. Because CH receives updated data of nodes every time. Scheduling necessary to slot assignment needed to watching of every watching node is no needed.

Let us compare energy consumption necessary to watching node in proposed method and previous method. Considering WSN consisting of N nodes, G=(V,E), the network is divided into $P_{opt}N$ clusters, where P_{opt} is a probability that CH is selected optimally. If the network is in $2a \times 2a$ sense field, P_{opt} is as follows.

$$P_{opt} = \left(\frac{1}{3c} + \frac{\sqrt[3]{2}}{3c(2+27c^2+3\sqrt{3}c\sqrt{27c^2+4})^{\frac{1}{3}}} + \frac{(2+27c^2+3\sqrt{3}\,c\sqrt{27c^2+4})^{\frac{1}{3}}}{3c} \cdot \frac{1}{\sqrt[3]{2}} \right)^2 \quad (12)$$

where $c = 1.53\sqrt{N}$.

Also, the maximum hopping number in one cluster is as follows.

$$K = \text{int}\left(\frac{1}{r}\sqrt{\frac{-0.017 \ln \frac{\alpha}{7}}{P_{opt} \cdot \lambda}} \right) + 1, \quad \lambda = \frac{N}{4a^2} \quad (13)$$

where αN is the number of overlapping clusters, r is the sense radius of node and k is usually 2~3.

That is, there are $P_{opt}N$ CHs, one cluster corresponding to them, at least more than $N_{WATCH,min}$ watching nodes when CH is different from watching node each other.

In this paper, we assume that one watching node watches $\overline{D}(G)$ sensor nodes all, as one watching node can watch $\overline{D}(G)$ targets at maximum. If watching node watches $\overline{D}(G)$ one's neighbor node v_j, communication energy consumed that node v_j watches is as follows, when the length of require message is L_{req} and the length of response message is L_{res}.

$$E_{i,WATCH}^i(i) = L_{req}E_{elec} + \varepsilon L_{req}d_{ij}^2 + L_{res}E_{elec} \quad (14)$$

where $L_{req}E_{elec} + \varepsilon L_{req}d_{ij}^2$ is energy consumed on transmitting require message and $L_{res}E_{elec}$ is energy consumed on receiving response message.

In this case, communication energy that node v_j consumed is as follows.

$$E_{i,WATCH}^{j}(j) = L_{req}E_{elec} + L_{res}E_{elec} + \varepsilon L_{res}d_{ij}^2 \tag{15}$$

Usually, $L_{req} < L_{res}$. The length of response message is 3~10 times longer than the length of require message, as the length of require message is same as the length of control message and the length of response message is same as the length of data packet.

That is, energy that node v_j watches is as follows.

$$E_{i,WATCH}^{i} = \sum_{v_j \in G_{WATCH,i}^{target}} E_{i,WATCH}^{i}(j) \tag{16}$$

The total communication energy that targets consumed is $\sum_{v_j \in G_{WATCH,i}^{target}} E_{i,WATCH}^{j}(j)$ and consumption of total communication energy is $E_{i,WATCH}^{i} + \sum_{v_j \in G_{WATCH,i}^{target}} E_{i,WATCH}^{j}(j)$.

The communication energy consumed on watching is as follows.

$$\begin{aligned} E_{WATCH,comm} &= \sum_{v_i \in G_{WATCH}} \left[E_{i,WATCH}^{i} + \sum_{j \in G_{WATCH,i}^{target}} E_{i,WATCH}^{j}(j) \right] = \\ &= \sum_{v_i \in G_{WATCH}} \sum_{v_j \in G_{WATCH,i}^{target}} \left[E_{i,WATCH}^{i}(i) + E_{i,WATCH}^{j}(j) \right] = \\ &= \sum_{v_i \in G_{WATCH}} \sum_{v_j \in G_{WATCH,i}^{target}} \left[2L_{req}E_{elec} + 2L_{res}E_{elec} + \varepsilon d_{ij}^2 (L_{res} + L_{req}) \right] \end{aligned} \tag{17}$$

where G_{WATCH} is a set of watching nodes in $G=(V,E)$.

$$E[d_{ij}^2] = \frac{2a^3}{3N_{WATCH,\min}N} \tag{18}$$

$$E_{WATCH,comm} = N_{WATCH,\min}\left(\frac{N}{N_{WATCH,\min}} - 1\right) \begin{bmatrix} 2E_{elec}(L_{req} + L_{res}) + \\ \varepsilon(L_{req} + L_{res})\dfrac{2a^3}{3N_{WATCH,\min}N} \end{bmatrix} \tag{19}$$

As shown in Eq.(19), energy consumed on watching depends on the length of require message, L_{req}, the length of response message, L_{res}, the number of watching nodes, $N_{WATCH,min}$, the number of sensor nodes, N, the size of sense field, $4a^2$.

Besides, it depends on energy consumed on transmitting and receiving one bit, E_{elec} and propagation coefficient ε, but these cannot be controlled, as these are fixed constants.

Energy consumed on calculation for watching is as follows.

$$E_{WATCH,cal} = K_{cal} \cdot L_{res} \cdot \left(N - N_{WATCH,\min}\right) \tag{20}$$

where K_{cal} is a coefficient.

Consequently, total energy consumption necessary to watching is as follows.

$$\begin{aligned} E_{WATCH,total} &= E_{WATCH,comm} + E_{WATCH,cal} = \\ &= (N - N_{WATCH,\min}) \begin{bmatrix} 2E_{elec} \cdot (L_{reg} + L_{res}) + \\ \varepsilon(L_{res} + L_{reg})\dfrac{2a^3}{3N_{WATCH,\min}N} + \\ K_{cal} \cdot L_{res} \end{bmatrix} \end{aligned} \tag{21}$$

If L_{res} is not smaller than L_{DATA} as the watching nodes have to decide the trust and response type of corresponding node based on data generated by target. In general, $L_{res}=L_{DATA}$ but $L_{res}>L_{DATA}$, as L_{res} is increased as necessary number of bits to transmit the second information, if the watching node is used to determine the trust of targets secondly.

The number of optimal clusters calculated without considering watching, $N \cdot P_{opt}$ is smaller than the minimum number of watching nodes, $N_{WATCH,min}$.

If $\overline{D}(G)$ is an average degree of network in $N_{WATCH,min}$, the degree of network in net is 4~8 and 6~12 in hexagonal.

P_{opt} is different with respect to N, about 0.1 for N = 500, 0.07 for N = 1000 and 0.05 for N=2000. That is, $N \cdot P_{opt} \approx N_{WATCH,min}$ for N = 100~500, $N_{WATCH,min}$ is 1.5~2 times larger than $N \cdot P_{opt}$ for $N \geqq 1000$.

If the probability that one sensor node is attacked during notice time T is $P_{attack}(T)$, the probability that this event is reported to CH directly is as follows.

$$\frac{NP_{opt}}{N_{WATCH,\min}} = P_{opt} \cdot \overline{D}(G) \tag{22}$$

Energy consumption when this event is reported to CH directly is as follows.

$$E_{attack}^{CH} = 2L_{res} \cdot E_{elec} + \varepsilon L_{res} \cdot \overline{D}^2_{hop} \tag{23}$$

where $\overline{D}_{hop} = E[d_{ij}^2]$.

The total energy consumption when this event is reported through relay node is as follows.

$$E_{attack}^{relay} = 2\overline{H} \cdot L_{res} \cdot E_{elec} + \overline{H} \cdot \varepsilon L_{res} \cdot \overline{D}^2_{hop} \tag{24}$$

That is, energy necessary to report data about sensor node that is attacked is as follows, considering the probability that is attack occurs.

$$\begin{aligned} E_{attack} &= NP_{attack}(T)\left(P_{opt}\bar{D}(G)E_{attack}^{CH} + \left[1 - P_{opt}\bar{D}(G)\right]E_{attack}^{relay}\right) \\ &= NP_{attack}(T)\left\{\begin{matrix} P_{opt}\bar{D}(G)\left[2L_{res}E_{elec} + \varepsilon L_{res}\overline{D}^2_{hop}\right] + \\ \left[1 - P_{opt}\overline{D}(G)\right]\left[2\overline{H}L_{res}E_{elec} + \overline{H}\varepsilon L_{res}\bar{D}^2_{hop}\right] \end{matrix}\right\} \\ &= NP_{attack}(T)\left\{\begin{matrix} 2L_{res}E_{elec} + \varepsilon L_{res}\bar{D}^2_{hop} + \left(1 - P_{opt}\bar{D}(G)\right)\cdot \\ \left[2L_{res}E_{elec}\left(\overline{H} - 1\right) + \left(\overline{H} - 1\right)\varepsilon L_{res}\bar{D}^2_{hop}\right] \end{matrix}\right\} \\ &= NP_{attack}(T)\left(2L_{res}E_{elec} + \varepsilon L_{res}\bar{D}^2_{hop}\right)\left[1 + \left(\overline{H} - 1\right)\left(1 - P_{opt}\bar{D}(G)\right)\right] \\ &= NP_{attack}(T)\left(2L_{res}E_{elec} + \varepsilon L_{res}\bar{D}^2_{hop}\right)\begin{bmatrix} \overline{H} - \overline{H}P_{opt}\bar{D}(G) \\ + P_{opt}\bar{D}(G) \end{bmatrix} \end{aligned} \tag{25}$$

$$P_{attack}(T) = \lambda_{attack} T \tag{26}$$

$$E_{attack} = N\lambda_{attack} T\left[2L_{res}E_{elec} + \varepsilon L_{res}\bar{D}_{hop}^2\right] \left[\bar{H} - \bar{H}P_{opt}\bar{D}(G) + P_{opt}\bar{D}(G)\right] \tag{27}$$

So, using CH and relay node as watching node consumes P_{attack} energy at most, instead of saving $E_{WATCH,min}$ at least compared with setting the watching node separately.

$$E_{WATCH,\min} = \left(N - N_{WATCH,\min}\right)\left[2E_{elec}\begin{pmatrix}L_{req}\\+L_{res}\end{pmatrix} + \varepsilon\begin{pmatrix}L_{req}\\+L_{res}\end{pmatrix}\bar{D}_{hop}^2\right]$$

$$= N\left(1 - \frac{N_{WATCH,\min}}{N}\right)\left[2E_{elec}(L_{req}+L_{res}) + \varepsilon(L_{req}+L_{res})\bar{D}_{hop}^2\right]$$

$$= N\left(1 - \frac{1}{\bar{D}(G)}\right)\left[2E_{elec}(L_{req}+L_{res}) + \varepsilon(L_{req}+L_{res})\bar{D}_{hop}^2\right]$$

$$> N\left(1 - \frac{1}{\bar{D}(G)}\right)\left[2L_{res}E_{elec} + \varepsilon L_{res}\bar{D}_{hop}^2\right]$$

$$> N\lambda_{attack} T\begin{bmatrix}\bar{H} - \bar{H}P_{opt}\bar{D}(G)\\+P_{opt}\bar{D}(G)\end{bmatrix}\begin{bmatrix}2L_{res}E_{elec}\\+\varepsilon L_{res}\bar{D}_{hop}^2\end{bmatrix} = E_{attack} \tag{28}$$

The problem determining the watching cycle is very important in security and energy efficiency. If the watching cycle is too long, it can't provide security, else, energy consumption is too large. In previous works [7], the watching cycle is determined as a function of trust, trust accuracy and trust robustness. In this way, the computation is large and synchronization in scheduling WSN can't be provided, if the watching cycle is changed continuously.

So, this method cannot be used in WSN using scheduling MAC protocol.

In this paper, we assume that the watching cycle in clustering WSN is same as the data gathering and environment watching cycle. The reason is as follows.

First, energy consumption is decreased, as the watching nodes do not need to wake up for only watching, if the watching cycle is same as the data gathering cycle.

Second, data gathering cycle and environment watching cycle is defined by the characteristics of target and environment, or system and they are set large enough that the frequency that can transmit the updated data compared with before. If the data cycle is shorter than watching cycle *V*, energy consumption is not efficient. If the watching cycle is integer times longer than the data cycle, the problem in security occurs, as reliability of corresponding data can't be estimated when reporting updated data. That is, we decrease energy consumption and the problem in security do not occur by setting the data cycle as watching cycle.

3. SIMULATION RESULTS

We compared energy consumption in case of watching by using the proposed method with energy consumption in case of watching by using the method in previous work with respect to the probability that attack occurs during given slot.

Table.1. shows simulation parameters

Parameters	Value
Network grid	100×100m
Number of nodes	100~1000
Length of Data, *n*	4000 bit (500byte)
Electronics energy, E_{elec}	50nJ/bit
Data Aggregation energy, E_{DA}	50nJ/bit
Transmitter energy, ε	10pJ/bit/m^2
Amplifier energy, ε_2	0.0013pJ/bit/m^4
Initial energy, E_{init}	0.5J
The length of data message to the length of control message ratio	3:1

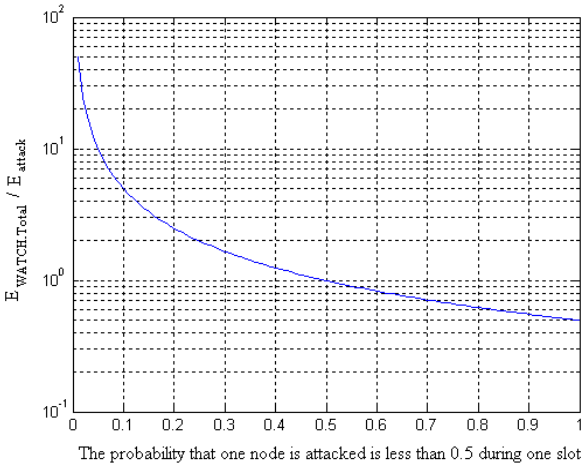

Fig.2. Ratio between energy consumption by using the proposed method and previous method versus the probability that attack occurs for *N*=100

As shown in Fig.2, the proposed method watches with smaller energy than the previous method when the probability that one node is attacked is less than 0.5 during one slot.

The reason is that energy consumption is independent of the probability that attack occurs, as the watching node has to watch periodically in previous method. However, in the proposed method, energy consumption on watching is small when the probability that attack occurs is small, as data gathering is watching and the information about attack only when the attack occurs is relayed.

The performance of the proposed method improves as the number of nodes increases. The reason is that the number of nodes belonging to one cluster increases, as the number of nodes increases. That is, energy consumption on watching is increased smaller than energy consumption by gathering in one cluster communication.

Simulation results show that using the proposed method in clustering WSN is superior to using the previous method. Although the performance seems low, when the probability that attack occurs is more than 0.5~0.8, however, in general case, the probability that attack occurs is lower than 0.01.

4. CONCLUSIONS

In previous works, they referred the watching attack of WSN of which topology is routing, but they have not referred the watching attack of WSN of which topology is clustering. First, we configure trust system and propose the optimization of watching node's position and watching period in clustering WSN in this paper. Second, we compare and analyze the proposed method and the method in routing WSN by mathematical modeling. Simulation results show that using the proposed method in clustering WSN is superior to using the previous method. Although the performance seems low, when the probability that attack occurs is more than 0.5~0.8, however, in general case, the probability that attack occurs is lower than 0.01.

REFERENCES

[1] S. Buchegger and J.Y. Le Boudec, "Performance Analysis of the Confidant Protocol: Cooperation of Nodes "Fairness In Dynamic Ad-hoc Networks", *Proceedings of IEEE/ACM Symposium on Mobile Ad Hoc Networks and Computing*, pp. 223-229, 2002.

[2] Q. He, D. Wu and P. Khosla, "SORI: A Secure and Objective Reputation-Based Incentive Scheme for Ad Hoc Networks", *Proceedings of International Conference on Wireless Communications and Networking*, pp. 745-753, 2004.

[3] P. Michiardi and R. Molva, "Core: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks", *Proceedings of International Conference on Advanced Communications and Multimedia Security*, pp. 107-121, 2002.

[4] Ismat K. Maarouf and A.R. Naseer, "WSNodeRater-An Optimized Reputation System Framework for Security Aware Energy Efficient Geographic Routing in WSNs", *Proceedings of IEEE/ACS International Conference on Computer Systems and Applications*, pp. 265-269, 2007.

[5] A. Perrig, J. Stankovic and D. Wagner, "Security in Wireless Sensor Networks", *Communications of the ACM*, Vol. 47, No. 6, pp. 53-57, 2004.

[6] M.L. Das, "Two-Factor User Authentication in Wireless Sensor Networks", *IEEE Transactions on Wireless Communications*, Vol. 8, No. 3, pp. 1086-1090, 2009.

[7] Jie Zhang, Jianying Zhou and Joseph Chee Ming Teo, "Toward Energy-Efficient Trust System through Watchdog Optimization for WSNs", *IEEE Transactions on Information Forensics and Security*, Vol. 10, No. 3, pp. 613-625, 2015.