International Journal of Security and Its Applications
Vol. 9, No. 6 (2015), pp. 19-34
http://dx.doi.org/10.14257/ijsia.2015.9.6.03

Epidemic Model based Security Analysis of Firefly Clock Synchronization in Wireless Sensor Networks

Zhiling Tang and Simin Li

Guangxi Key Laboratory of Automatic Detecting Technology and Instruments (Guilin University of Electronic Technology), Guilin 541004, P.R.China
tzl888@guet.edu.cn

Abstract

This paper discusses the security of the clock synchronization algorithm based on the biological example of Asian Fireflies in wireless sensor networks. Huge swarms of these fireflies use the principle of pulse coupled oscillators in order to synchronously emit light flashes to attract mating partners. When applying this algorithm to real sensor networks, the potential threat of hostile flashes may disturb this synchronization. An improved Reachback Firefly Algorithm is implemented in the MAC layer of wireless sensor networks (WSNs), which change coupling strength among oscillators to anti hostile attack in clock synchronization. Its security is analyzed through a Susceptible-Infective-Recovered epidemic model. Numerical results and simulations are provided for further understanding of the analysis.

Keywords: *SIR epidemic model; synchronization; Firefly Algorithm; security analysis*

1. Introduction

Clock synchronization is a key technique for wireless sensor networks (WSNs) because data sensed by each sensor must be obtained at same time in many cases. For example, Nunez *et al.*, demonstrate that decreasing synchronization error of sampling clocks in an audio sensor network which estimates the location of a sudden and loud noise accurately can improve the triangulation accuracy [1]. The triangulation algorithm utilizes the difference in time of arrival to each audio sensor. Experiment of [1] shows that the triangulation accuracy is worse when the error is more than $13\mu s$.

Clock synchronization is beneficial to extend the battery life of a wireless sensor node. In WSNs, a node takes up most of time to receive radio signal. In order to reduce energy cost, one feasible method is to intelligently make a node enter into sleep mode during which the node turns off its radio receiver [2]. Though it is a complicated control process for this distributed system, there is a simple strategy if this system has synchronized clock. Once the system is synchronized, a node is only waked up during a specified time-slot. In this case, clock synchronization is a basic technique assures that all other nodes know when to power up their radio receiver [3].

In addition, clock synchronization is useful for cooperative communication of WSNs [4]. A group of nodes send same signal at the same time, so the total transmitted power is larger which make signal propagate further. But total signal is enhanced only when all nodes transmit signal having same frequency and phase. In order to satisfy this condition, all nodes must be synchronized.

Different methods have been proposed to synchronize each node's clock. The one of the most suitable for distributed networks is Firefly algorithm, on which Pulse Coupled Oscillator (PCO) is based. The results in [5] inspired Hong and Scaglione into doing the experiment of PCO in WSNs [6]. The experiment shows that this method is inherently decentralized and resilient to individual node failure. Geoffrey Werner-Allen et al. present the Reachback Firefly Algorithm (RFA) which is also based on PCO [7]. Some problems

ISSN: 1738-9976 IJSIA

existing in realistic WSNs, such as message delays and loss, are considered. The algorithm overcomes these problems by using past delayed information to adjust the future firing phase. The experiment with TinyOS-based nodes proves the convergence of the algorithm in simple cases, and all nodes can be synchronized within 100μs on a real multi-hop topology with links of varying quality.

The security of WSNs is considered recently. In some cases, hostile nodes access into networks in order to make WSNs lose its efficacy. For example, the attack of worms is a major issue these days in WSNs [8]. Because of the publicity of wireless transmission medium, WSNs is vulnerable to various security threats. The broadcast nature of wireless communication provides a way to spread malicious code in the network. Several malicious codes target the wireless network through different portable devices like laptops, smart phones and tablets. For the security of clock synchronization in WSNs, a cluster-based secure synchronization protocol (CLUSS) is proposed [9]. The process of CLUSS comprises three stages: authentication phase, inter-cluster synchronization phase and intra-cluster synchronization phase. This synchronization protocol provides security with the authentication to traditional beacon-based synchronization. For Firefly synchronization algorithm, it is necessary to discuss its ability of recovery when the synchronization is attacked by hostile nodes. In this paper, the attack to Firefly synchronization algorithm including attacking methods and attacking consequences is analyzed by epidemic model. Then its ability of recovery is discussed and proved by simulation.

The rest of this paper is organized as follows. In Section 2, the theory of firefly algorithm and its several ways of implementation are described. But these ways are not easy to implement on current hardware platforms of WSNs. Then a method which is suitable for WSNs, called as Reachback Firefly Algorithm, is introduced in Section3. Based on analysis of its working process for synchronization, we propose an improvement for it. According to the analysis, we establish a model of the improved algorithm with epidemic theory in Section 4. Numerical methods are employed to simulate the dynamic behavior of the epidemic model to verify its ability of anti attack. Finally, we give the conclusion of our article in Section 6.

2. Related Work

PCO originated from synchronous flashing of fireflies. The mechanism behind this phenomenon observed by Blair in 1915 has been investigated for nearly a century. Blair analogize firefly to electric battery--each flash temporarily exhausts the battery, and a period of recuperation is required before the next flash can be emitted. A leader's flash excites the discharge of others. Eventually all the fireflies flash in concert [10]. In 1988, Buck proposed the phase-advanced model. There is a "late sensitivity window" as a time interval during the period between a firefly's flashings. When a flash occurs during the late sensitivity window, it initiates an immediate flash and resets the status of the firefly. Although this model gives a fine explanation to some varieties of fireflies' synchronization behavior, the interaction, which is usually called coupling, between fireflies is narrowly limited to late sensitivity window. Peskin extended coupling to any time of the cycle [11]. In his book published in 1975 [11], Peskin proposed a more detailed pulse-coupled oscillators model for the natural pacemaker of a human heart. He modeled a pacemaker as a system consisting of mutual coupled "integrate-and-fire" oscillators. The state function in the Peskin's model is the well-known leaky integrate-and-fire model which is defined as

$$\frac{dx_i(t)}{dt} = S_0 - \gamma x_i(t), \quad 0 < x(t) < 1 \quad i = 1,...,N \tag{1}$$

where S_0 is a constant meaning the speed of accumulation when there are no leakage , γ is the leakage factor. From (1), we can obtain

$$f(\phi) = C(1 - e^{-\gamma T\phi}) \tag{2}$$

where $C=1/(1-e^{-\gamma T\phi})$ and $T = \gamma^{-1}\ln[S_0/(S_0-\gamma)]$. The actual implementation of Peskin-type PCO is a simple *RC* circuit shown as Figure 1, where the constant charge S_0 and the leaking component $-\gamma T\phi$ are sent into the integrator. A pulsing occurs when $x_i(t)$ reaches the threshold 1. The pulsing is expressed by the Dirac delta function $|(dx(t)/dt)|\delta[x(t)-1]$, which integrates to 1 with respect to t after the time t^*, where $x(t^*)=1$.

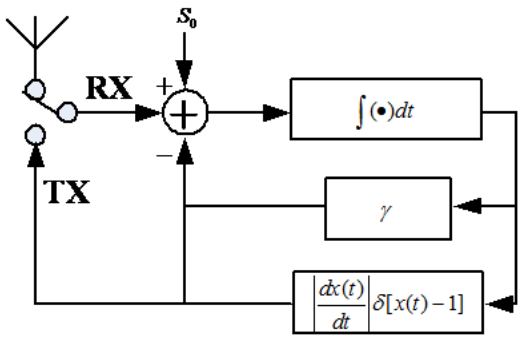

Figure 1. Peskin's Integrate-and-fire Model [5]

Then, Mirollo and Strogatz [5] give one of the earliest complete analytical studies of PCO systems. In their model, every oscillator has a fixed time period T and its time or phase t, which starts from zero to T at a constant rate. At time $t=T$, the oscillator A flashes and resets $t=0$. All oscillators may not start at the same time, so their internal time t is not synchronous. In the absence of any input from neighbors, the oscillator B simply flashes whenever $t=T$. If B sensing a neighbor flashes, it will adjust phase forward which shorten its own time to flash (Figure 2 (a-b)). The amount of adjustment is determined by the flashes function $f(t)$. If the time of the oscillator B senses a neighbor flashes at $t=t'$, the oscillator B instantaneously jumps to a new internal time $t=t"$ where

$$t"=f^{-1}(f(t')+\varepsilon) \tag{3}$$

If $t">T$, $t=T$ and immediately flashes and resets $t=0$.

However, above methods are impractical when used on WSNs in which a node acts as an oscillator. Hong and Scaglione's algorithms depend on specific electronic circuit to implement PCO [6], so it is not easy to implement on current WSN hardware platform. Mirollo and Strogatz's (M&S) model assumes that all nodes work on condition of lossless radio links. All nodes have identical oscillator frequencies and the ability of arbitrary-precision floating-point arithmetic. In the real environment of WSNs, radio contention and message processing lead to significant and unpredictable communication latency. In order to resolve these problems, Reachback Firefly Algorithm [7] implemented on MAC layer utilizes past delay error to adjust future flashing phase. It tackles these problems in four aspects. Firstly, low level timestamp is used to estimate the delay time of a message before it is broadcasted. Secondly, the oscillator algorithm is modified by the notion of "reachback", which means that a oscillator reacts to messages from the previous time period rather than the current time period. Thirdly, messages are staggered to avoid the worst case of wireless contention. Lastly, a simple and approximate flashing function that can be computed quickly is used. The process of adjusting phase is shown as Figure 2 (c).

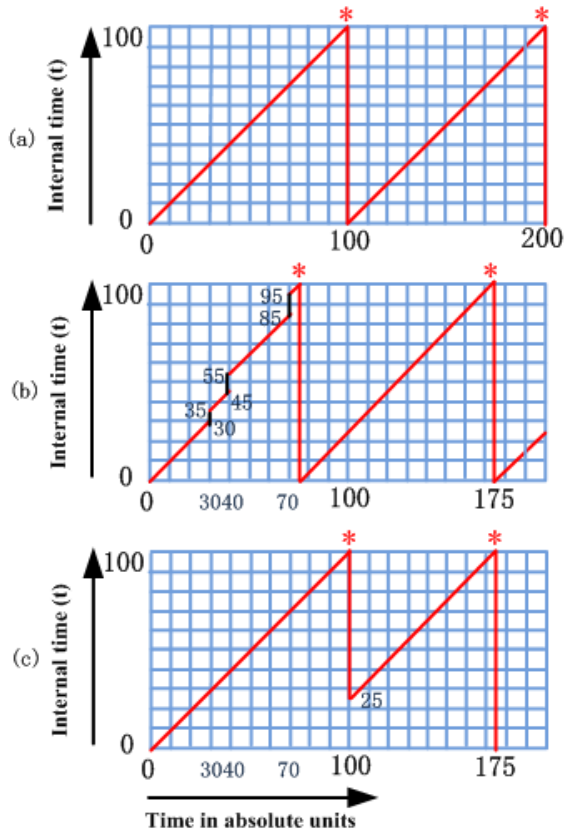

Figure 2. Firefly-inspired Synchronization Algorithm. (a) An Oscillator Flashes Whenever its Internal Time t is Equal to the Default Time Period T (=100). (b) In the M&S Model, an Oscillator Responds to Neighbors Firing (Arrows) by Instantaneously Incrementing t. (c) In RFA, an Oscillator Records the Flashing Events and Responds all at once at the beginning of the Next Cycle [7]

Although Reachback Firefly Algorithm which implements PCO on MAC layer has run on TinyOS-based node of WSNs, its security remains to be verified.

3. Security Analysis of Synchronization Algorithm

WSNs must have the ability of anti attacks because of the openness of wireless communication channel. These attacks always exploit WSNs' weakness to make its work fail. Since Firefly Algorithm based synchronization depends on wireless communication, the attack to wireless channel may lead to the failure of synchronization. The process of synchronization between two oscillators is analyzed to show the weakness of the algorithm. Then the improvement of Reachback Firefly Algorithm is described.

3.1. Process of Synchronization between Two Oscillators

First the working scene is defined. Let the clock cycle T=100 time units. The oscillator B starts at internal time t=0 and increases t every unit time. It is supposed that firing events occurs at absolute times 30, 40 and 70. Let $\Delta(t)$ be jump function representing the instantaneous jump at internal time t .

If the M&S model used, when a message is received instantaneously, an oscillator reacts instantaneously as shown in Figure 2(a-b). Once the oscillator B observed a flash at

time t=30 , it computes an instantaneous hop of $\Delta(30)=5$, and sets $t=30+\Delta(30)=35$. Ten more time units from this point there is another event at 40 units of time since the beginning of the cycle. The oscillator perceives it as having happened at internal time $t=45$. The node again computes an instantaneous jump in internal time $t=45+\Delta(45)=55$. After 30 more time units another flashing is observed by the oscillator B. At this point $t=85$ and the oscillator computes an instantaneous hop to $t=85+\Delta(85)=95$. After 5 more time units, $t=100$ and the oscillator B flashes.

By contrast, Reachback Firefly Algorithm does not react instantaneously shown as Figure 2(c). At first the delay between the time when an oscillator flashes and the time when the message is transmitted is estimated. So a MAC-layer time-stamp is used to record the delay experienced in MAC layer by a message prior to transmission. The measurement is triggered by an event when the message is about to be transmitted, and is recorded in the header of the outgoing message. When an oscillator receives a flashing message, it extracts this information to determine the correct flashing time by subtracting the delay in MAC layer from the time when the message is received. This method of estimating message transmission delay is similar to FTSP [12]. Next, the oscillator B does not react instantaneously when it observes the oscillator A's flashing. It produces a reachback response, which put the message in a queue when it sensed a neighbor flash. The message is embedded with timestamp of correct internal time t' when the flashing event occurred. When the node reaches the time t=T , it flashes. Then it "reaches back in time" by looking at the queue of messages received during the past period. Based on those messages, it computes the overall jump and increments t immediately shown as Figure 2(c). In order to avoid channel collision induced by flash, CSMA schemes add a random transmission delay to an oscillator flashing message at the application layer. The delay is uniformly random between 0 and a constant D. After a oscillator flashes, it waits for a grace period W (where $W>D$ and W □ T) before processing the queue so that delayed messages from synchronized oscillators are received. This algorithm uses a simple flashing function $f(t)=\ln(t)$ to speed flashing response. Substituting the equation $f^{-1}(x)=e^{x}$ to (3), the increment of a hop in response to a flashing event is $\Delta(t')=f^{-1}(f(t')+\varepsilon)-t'=(e^{\varepsilon}-1)t'$. First order of Taylor expansion e^{ε}=1+ε is a simple way to calculate the jump.

$$\Delta(t')=\varepsilon t' \tag{4}$$

According to the theory of Reachback Firefly Algorithm, the process of synchronization between the oscillator A and the oscillator B is described as follows. Two oscillators can be look as two points moving alone the curve $s=f(\phi)$ at a constant horizontal velocity 1/T shown as Figure 3. When the oscillator A's time $\phi=1$, its flash occurs and is recorded by the oscillator B. As shown in Figure 4, the time when A flashes recorded by B is ϕ_B, and A jumps to ϕ_A. After that, both oscillators move forward in their cycles until B s. After B flashed, B jumps to phase $\Delta(\phi_B)$. The hop is defined as $\Delta(\phi_B)$=$g(f(\phi_B)+\varepsilon)-\phi_B$, where g=f^{-1} and ε □ 1. At the same time, A has advanced a distance $1-\phi_B$, running up to the phase ϕ_A+$1-\phi_B$, and recording this as B's last flashing time. So when A finishes its next flash, it will jump to $\Delta(\phi_A+1-\phi_B)$. Then B is at $\Delta(\phi_B)+1-(\phi_A+1-\phi_B)=\Delta(\phi_B)-\phi_A+\phi_B$. The flashing time of two oscillators obey following iteration:

$$\begin{bmatrix}\phi_A\\ \phi_B\end{bmatrix}_{n+1}=\begin{bmatrix}e^{\varepsilon}-1 & -(e^{\varepsilon}-1)\\ -1 & e^{\varepsilon}\end{bmatrix}\begin{bmatrix}\phi_A\\ \phi_B\end{bmatrix}_{n}+\begin{bmatrix}e^{\varepsilon}-1\\ 0\end{bmatrix} \tag{5}$$

where n is the cycle number. The equation (5) is a linear dynamic system $\vec{\phi}$, where $\vec{\phi} \in [0,1]\times[0,1]$. The unique fixed point of this dynamical system is easily proven to be $\vec{\phi}^* = [0,1/2]^T$. Let $\vec{\varphi}_n = \vec{\phi}_n - \vec{\phi}^*$, (5) is rewrote as

$$\vec{\varphi}_{n+1} = M\vec{\varphi}_n \tag{6}$$

By the eigen-decomposition of M, it is decomposed as $M = V\Lambda V^{-1}$, where V is matrix of eigen-vectors and Λ is diagonal matrix. Its eigen-value is ε^2 and $1+\varepsilon$. It is not difficult to prove that the matrix M is convergent when $n \to \infty$, and the unique fixed point is $[0,0]^T$ or $[1,1]^T$. This means two oscillators are synchronous.

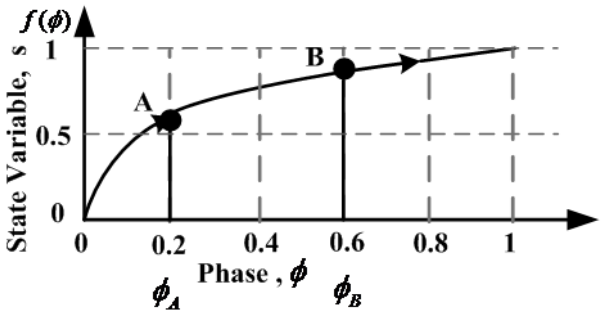

Figure 3. Two Nodes A and B Moving Along $s = f(\phi)$ [7]

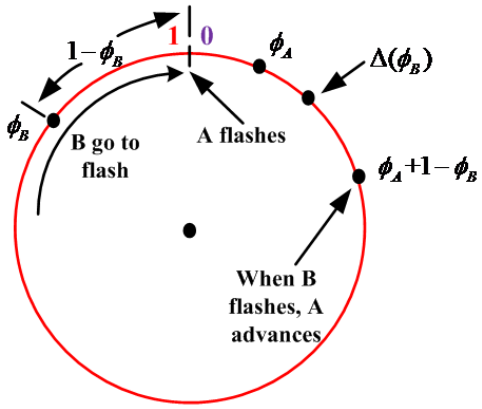

Figure 4. Iteration between the node A and the node B

It is obvious that the synchronization of two oscillators utilizes coupling effects on their clock. Because their coupling pass through open wireless channel which can be accessed by anyone, flashes generated by hostile nodes can be propagates to any nodes. Song H. et al. concluded that there are 4 attacks to clock synchronization in WSNs [13]: the masquerade attack, the replay attack, the message and the manipulation attack. But these attacks are implemented on the application layer. The attack to synchronization based on Reachback Firefly Algorithm is different because the synchronization is fulfilled on the MAC layer. The process of the attack is described as follows.

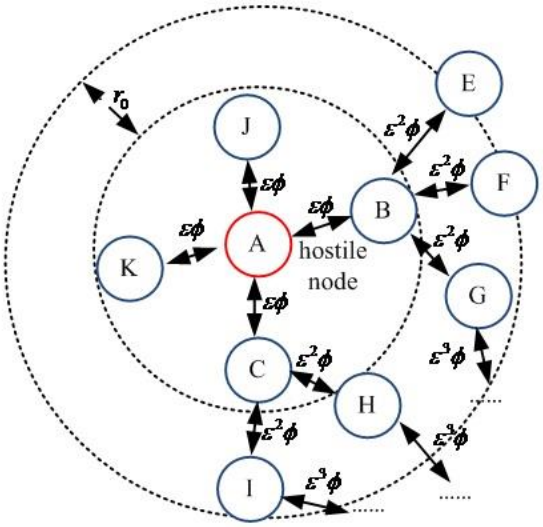

Figure 5. Hostile Message Spreads via Open Wireless Channel

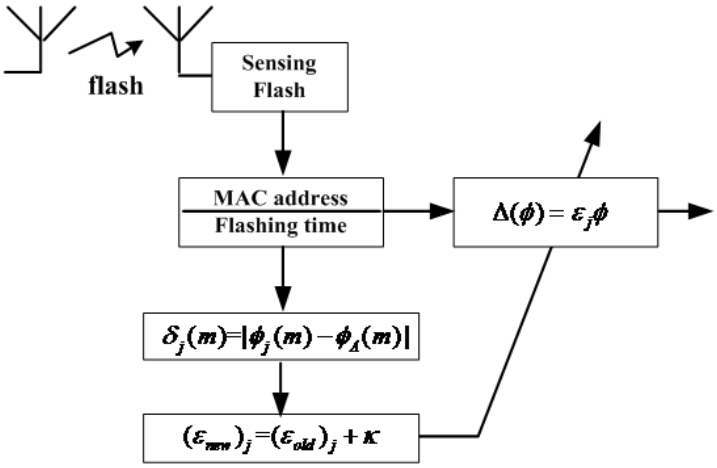

Figure 6. Adaptive Coupling Strength Adjustment

Here nodes in WSNs are look as oscillators. The hostile oscillator flashes at random interval to its neighbor oscillators in order to make them be out of synchronization. The oscillator B will record this time and jumps to certain initial phase in next period once it received the hostile oscillator's flash. Because flash events occur randomly, the period of the oscillator B is not convergent. Then the oscillator B's flashes makes its neighbor oscillators change their phase again. As shown in Figure 5, the same change is copied by more oscillators. Although the initial jumping phase of an oscillator is determined by its all neighbor oscillators, the hostile oscillator will act as a major role if it flashes at the maximum difference in phase. From (4), the bigger t' is, the bigger $\Delta(t')$ is. Although this hostile coupling effect is attenuated by $\varepsilon^n(\varepsilon << 1)$ which limits the hostile action in a small area when it is propagated, some oscillators inevitably are out of synchronization or produce clock jitter. The hostile coupling effect of multi-hop is defined as follow:

$$\Delta(\phi_k) = \varepsilon^k \phi_k \tag{7}$$

where k is the number of hops. The value of ε is key to control the speed of WSN's clock synchronization. From [5] and [7], we obtain

$$k = \frac{1}{\ln(1+\varepsilon)} \ln(\frac{1}{2\delta - 1}) \approx \frac{1}{\varepsilon} \ln(\frac{1}{2\delta - 1}) \quad (8)$$

where k is the number of iterations required. Thus, the time to synchrony is inversely proportional to ε which is called as coupling strength.

3.2. Improvement of Synchronization Algorithm

In order to improve the security of the clock synchronization in WSN, an adaptive adjustment of ε to control the couple strength is proposed. In an oscillator's MAC layer, a monitor is used to analyze flash events of neighbor oscillators shown as Figure 6. When the oscillator B received the oscillator A's flashing message, it records MAC address of the message and the flashing time. Then the monitor in the MAC layer of the oscillator B computes the phase difference $\delta_j(m)$ between the oscillator A and other neighbor oscillators, which is

$$\delta_j(m) = |\phi_j(m) - \phi_A(m)| \quad (9)$$

where m is the number of the flashing sequence, j is the index of neighbor oscillators. The monitor compare $\delta_j(m)$ $(m = 1, ..., N)$ belong to the j th neighbor oscillator, where N is the number of certain neighbor oscillator's records. If the $\delta_j(m)$ has a trend of reduction, ε is updated by a new value which is as follows:

$$(\varepsilon_{new})_j = (\varepsilon_{old})_j + \kappa \quad (10)$$

where κ is the adjustment step size of ε. Otherwise,

$$(\varepsilon_{new})_j = (\varepsilon_{old})_j - \kappa \quad (11)$$

If a hostile oscillator disguises as a normal oscillator at first, its reciprocal ε would be maximum value. When it delivers an attack, its neighbor oscillators would be out of synchronization. But when its neighbor oscillators detect this abnormal case by their monitor, they will decrease their coupling strength as (11). So this adaptive mechanism provides a buffer for an oscillator to anti attack.

4. Epidemic Model of Synchronization Algorithm

In order to analyze the security of the improved Firefly Algorithm for synchronization, its epidemic model is established.

4.1. Improvement of Synchronization Algorithm

Epidemic theory has been used to study the infectious outcomes among a population with a susceptibility factor in respect of the infection [14]. Agent, Host and Environment are three variables to be considered in epidemic theory. Each variable has many manifestations. Not only communication between host and agent change has many ways, but also various environmental condition influences the interaction in innumerable ways. For instance, the agent is the individual who has an influenza virus in the study of influenza. The virus spread out via direct contact, or by way of a medium such as water, food, milk, or contaminated air. When an infectious agent invades a host, the host may become an agent because of infection. But if the agent is vaccinated, it may recover from the infection and become immune to future infections.

The characteristic of immunity may be temporary, long-lasting or permanent. There are various epidemic models such as Susceptible Infective Susceptible (SIS) model [15] and Susceptible Infective Recovered (SIR) model [16, 17] which characterize an infection spread. These models have been applied by epidemiologists, social and behavioral scientists in their research areas.

4.2. SIR Model of Improved Firefly Algorithm

Let $s(t)$, $i(t)$ and $r(t)$ express the number of susceptible, infective and recovered (or immune) oscillators respectively at time t. Let the total population be expressed by the constant N, then $N = s(t) + i(t) + r(t)$.

The radio coverage of a node in WSNs is πr_0^2. If the distribution density is ξ and the distribution is randomly uniform. The number of nodes which can received the flashing message is $\xi\pi r_0^2$. But not all nodes received the flashing message are infected because some of nodes have immunity and there is a buffer in MAC layer. All neighbor nodes can be divided into three groups, which are susceptible neighbors, infected neighbors and recovered neighbors. Only a susceptible neighbor of the infected node may become a new infected node. An infected neighbor or a recovered neighbor is not able to change a node's status when it received a hostile flashing message, since a node is either already infected or is immune to infection.

Let the infection capacity be expressed by η, which represents the probabilistic rate of a node being out of synchronization by a hostile flash from an infected node to a susceptible node. It is obvious η depends on the infectivity of a hostile flash. Let γ signify the recovery capacity, which is the probabilistic rate at which an infected node recovers and becomes immune. When a node is out of synchronization, a process of its remedy is automatically triggered by its MAC monitor. According to the predefined adjusting step size of ε, a fraction of the adaptively adjusted infected nodes will be cured and become recovered nodes. Because recovered nodes have identified the hostile node, they have the immunity from that hostile flashing message. The remainder of these nodes will remain in the group of infected nodes.

Basic differential equations that describe change rates of susceptible, infected, and recovered nodes are described as follows:

$$\begin{cases} \dfrac{di(t)}{dt} = \eta i(t)\dfrac{\xi\omega\pi r_0^2}{N} s(t) - \gamma i(t) \\ \dfrac{ds(t)}{dt} = -\eta i(t)\dfrac{\xi\omega\pi r_0^2}{N} s(t) \\ \dfrac{dr(t)}{dt} = \gamma i(t) \end{cases} \tag{12}$$

The initial conditions of (12) is

$$s(0) = N - 1, i(0) = 1, \text{ and } r(0) = 1 \tag{13}$$

As shown in Figure 5, the hostile flash 'illuminates' the area of radius $r(t)$ at time t, and other nodes within the area give no hostile flash. Then, the number of susceptible nodes and the number of infected nodes are given respectively as follows

$$s(t) = N - \omega\xi\pi r(t)^2 \tag{14}$$

$$i(t) = \omega\xi\pi r(t)^2 - \omega\xi\pi[r(t) - r_0]^2 - \gamma i(t) \tag{15}$$

where ω is represent how much the coupling strength ε is attenuated by MAC layer. From (14) and (15), we obtain

$$i(t) \approx \frac{2r_0\sqrt{\omega\xi\pi}}{1+\gamma}\sqrt{N - s(t)} \tag{16}$$

When (12) is substituted into (16) with the initial condition (13), the number of susceptible nodes is following equation.

$$s(t) = N - N(\frac{2}{1+Y_0 e^{-Y_1 t}} - 1)^2 \tag{17}$$

where $Y_0 = \frac{\sqrt{N}-1}{\sqrt{N}-1}$, and $Y_1 = \frac{2\eta(r_0\sqrt{\omega\xi\pi})^3}{(1+\gamma)\sqrt{N}}$. From (12), we obtain

$$\frac{di(t)}{ds(t)} = -1 + \frac{\gamma N}{\eta\omega\xi r_0^2}\frac{1}{s(t)} \tag{18}$$

When the initial condition is substituted into (18), $i(t)$ is resolved out as follow:

$$i(t) = N - s(t) - \frac{\sigma N}{\eta\omega\xi\pi r_0^2}\ln(\frac{N-1}{s(t)}) \tag{19}$$

where $\sigma = \gamma + p$ is called the total recovery capacity. When (17) is substituted into (19), the expression of $i(t)$ is obtained, and $r(t)$ is directly wrote as

$$r(t) = \frac{\sigma N}{\eta\omega\xi\pi r_0^2}\ln(\frac{N-1}{s(t)}) \tag{20}$$

Then the dynamics of $r(t)$, $s(t)$ and $i(t)$ are obtained.

When a node received a hostile flashing message, it is out of synchronization and copies the attenuated error to its neighbors by its next flash. Hence, the number of infected nodes will gradually increase. Simultaneously, their recovery mechanism triggered by the monitor will make the number of infected nodes decrease. Therefore, $i(t)$ will reach its maximum value represented by $i_m(t)$ at some point.

From (18), following equation is obtained when $di/ds = 0$:

$$s(t) = \frac{\sigma N}{\eta\omega\xi\pi r_0^2} \tag{21}$$

Since $d^2i/d^2s = -\frac{\sigma N}{\eta\omega\xi\pi r_0^2}\frac{1}{s^2} < 0$, $i(t)$ reaches a maximum value when $s(t) = \frac{\sigma N}{\eta\omega\xi\pi r_0^2}$.

From (17) and (21), the time when $i(t)$ reach its maximum value is

$$t = \frac{1}{Y_1}\ln(\frac{Y_0}{Y_2 - 1}) \tag{22}$$

where $Y_2 = 2/(1+\sqrt{1-\sigma/(\eta\xi\pi r_0^2)})$. So the time when $i(t)$ reaches the maximum value i_m is determined by (22).

5. Numerical Simulation

A numerical simulation based on the epidemic model is carried on for analyzing the security of synchronization of WSNs. The number N of nodes in WSNs is 1000 in simulation. These nodes are distributed uniformly in a circle. The characteristics of synchronization are obtained by changing the radius of the infection capacity η, the recovery capacity γ, the circle r_0, the distribution density ξ and the attenuation factor ω. In order to simplify expression, all parameters are given in dimensionless units.

At first, the time-varying process of the number of nodes which is out of synchronization is simulated. Simultaneously, the time-varying process of the number of susceptible nodes is simulated. The curves of $i(t)$ with time under different condition of η and γ are shown as Figure 7. The curves of $s(t)$ with time under different condition of η and γ are shown as Figure 8. $i(t)$ increases with time in the beginning. After it reaches a maximum point, it decreases gradually. While $s(t)$ decreases monotonously to zero. When η=0.8, the outbreak of infection is smaller, and the outbreak point is achieved earlier with the recovery capacity γ increasing. But under the same conditions, the curves of $s(t)$ are not changed. It is must be reminded that $s(t)$ = 0 does not mean a synchronization failure since an infection process often accompanies a recovery process. When γ=0.01, the outbreak of an infection is greater, and the outbreak point is achieved later with the infection capacity η increasing. While under the same conditions, $s(t)$ decreases more quickly since more susceptible nodes are infected. Therefore, it is ought to select smaller value of γ and greater value of η in order to decrease infected nodes and the error of synchronization. But the greater the value of η is, the more nodes are susceptible.

Secondly, the simulation similar to previous one are carried when the density ξ and the radius r_0 are changed. The curves of $i(t)$ with time under different condition of ξ and r_0 are shown as Figure 9. The curves of $s(t)$ with time under different condition of ξ and r_0 are shown as Figure 10. $i(t)$ increases with time in the beginning also. After it reaches a maximum point, it decreases gradually. While $s(t)$ decreases monotonously to zero. When ξ=0.5, the outbreak of infection is greater, and the outbreak point is achieved earlier with the radius r_0 increasing. While under the same conditions, $s(t)$ decreases more quickly since more susceptible nodes are infected. When r_0=6, the outbreak of an infection is greater, and the outbreak point is achieved earlier with the density ξ increasing. While $s(t)$ declines more quickly with the density ξ increasing. It is show that the outbreak point will come earlier if the distribution of node is more intensive or the radius is greater.

It is show that the synchronization of WSNs based on improved Firefly Algorithm is safe because the number of nodes which are out of synchronization decrease with time. The difference under various conditions is the time to recovery.

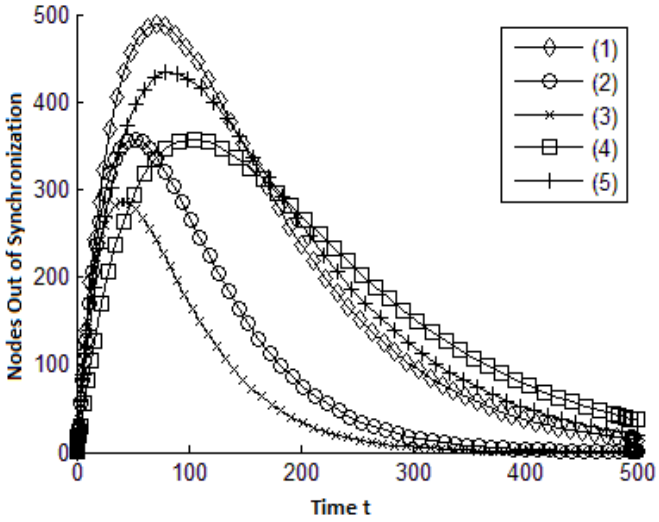

Figure 7. Transient Response of $i(t)$ with Regard to η and γ. (1) η=0.8，γ=0.01; **(2)** η=0.8，γ=0.02; **(3)** η=0.8，γ=0.03; **(4)** η=0.4，γ=0.01; **(5)** η=0.6，γ=0.01

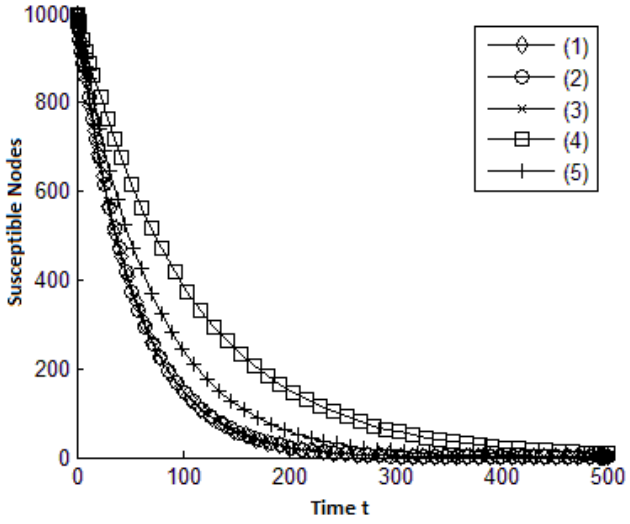

Figure 8. Transient Response of $i(t)$ with regard to η and γ. (1) η=0.8，γ=0.01; **(2)** η=0.8，γ=0.02; **(3)** η=0.8，γ=0.03; **(4)** η=0.4，γ=0.01; **(5)** η=0.6，γ=0.01

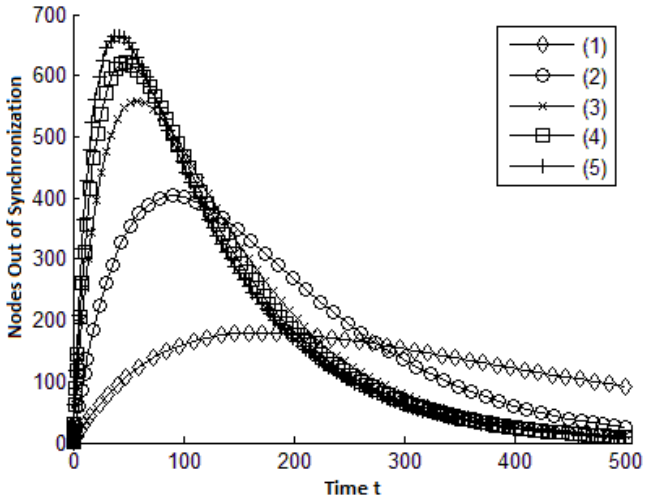

Figure 9. Transient Response of $i(t)$ with Regard to ξ and r_0. (1) ξ=0.5, r_0=2; (2) ξ=0.5, r_0=4; (3) ξ=0.5, r_0=6; (4) ξ=0.7, r_0=6; (5) ξ=0.9, r_0=6

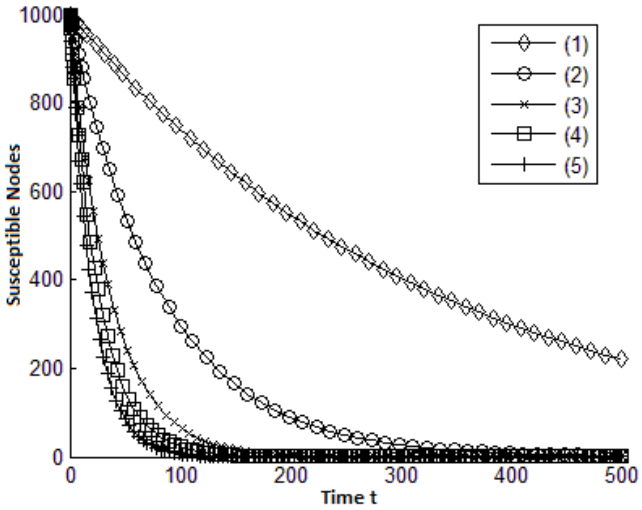

Figure 10. Transient Response of $s(t)$ with Regard to ξ and r_0. (1) ξ=0.5, r_0=2; (2) ξ=0.5, r_0=4; (3) ξ=0.5, r_0=6; (4) ξ=0.7, r_0=6; (5) ξ=0.9, r_0=6

6. Conclusion

This paper analyzes the security of the clock synchronization algorithm based on the biological example of Asian Fireflies in WSNs by epidemic model. The theory of the Firefly Algorithm is discussed by comparing its several schemes. Some potential threats to Firefly Algorithm are point out by our analysis. For Reachback Firefly Algorithm which is implemented in the MAC layer of WSNs, it is easy to be disturbed by hostile random flashes. An improved Reachback Firefly Algorithm is proposed by us, which used a monitor in MAC layer to analyze flash events of

neighbor oscillators. When the abnormal case induced by attack is detected, the coupling strength between nodes, also look as oscillators, is adjusted to buffer the attack. The security of improved Reachback Firefly Algorithm is analyzed by classical Susceptible-Infective-Recovered model. Through numerical simulation, it is show that the synchronization of WSNs based on improved Firefly Algorithm is safe because the number of nodes which are out of synchronization decrease with time. The difference under various conditions is the time to recovery. It is show that the outbreak point will come earlier if the distribution of node is more intensive or the radius is greater. In addition, It is ought to select smaller value of γ and greater value of η in order to decrease infected nodes and the error of synchronization. But the greater the value of η is, the more nodes are susceptible. Thus, future work is study the optimization algorithm to decrease the time to recovery with fewer susceptible nodes.

Acknowledgements

This project supported by the national natural science foundation of China (Grant No. 61461013).

References

[1] F. Nunez, Y. Wang, S. Desai, G. Cakiades and F. J. Doyle, "Bio-inspired synchronization of wireless sensor networks for acoustic event detection systems", IEEE Symposium on Precision Clock Synchronization for Measurement Control and Communication, Burlingame, **(2012)**, pp. 1–6.
[2] J. Podpora, L. Reznik and G. Von Pless, "Intelligent real-time adaptation for power efficiency in sensor networks", IEEE Sensors Journal, vol. 8, no. 12, **(2008)**, pp. 2066-2073.
[3] X. Wang, R. K. Dokania and A. Apsel, "PCO-Based Synchronization for Cognitive Duty-Cycled Impulse Radio Sensor Networks", IEEE Sensors Journal, vol. 11, no. 3, **(2011)**, pp. 555-564.
[4] H. Wan, J.-F. Diouris and G. Andrieux, "Time Synchronization for Cooperative Communication in Wireless Sensor Networks", Wireless Personal Communications, vol. 63, no. 4, **(2012)**, pp. 977-993.
[5] R. E. Mirollo and S. H. Strogatz, "Synchronization of pulse-coupled biological oscillators", SIAM J. Appl. Math., vol. 50, no. 6, **(1990)**, pp. 1645-1662.
[6] Y. W. Hong and A. Scaglione, "Time synchronization and reach-back communications with pulse-coupled oscillators for UWB wireless ad hoc networks", IEEE Conference on Ultra Wideband Systems and Technologies, Reston, **(2003)**, pp. 190-194.
[7] G. Werner-Allen, G. Tewari, A. Patel, M. Welsh and R. Nagpal, "Firefly-Inspired Sensor Network Synchronicity with Realistic Radio Effect", Proceedings of the 3rd international conference on Embedded networked sensor systems, San Diego, **(2005)**, pp. 142-153.
[8] B. Kumar Mishra, S. Kumar Srivastava and B. Kumar Mishra, "A quarantine model on the spreading behavior of worms in wireless sensor network", Transaction on IoT and Cloud Computing, vol. 2, no. 1, **(2014)**, pp. 1-13.
[9] M. Xu, G. Liu, D. Zhu and H. Wu, "A Cluster-Based Secure Synchronization Protocol for Underwater Wireless Sensor Networks", International Journal of Distributed Sensor Networks, vol. 2014, **(2014)**, Article ID 398610.
[10] K. G. Blair, "Luminous Insects", Nature, vol. 96, no. 2406, **(1915)**, pp. 411–415.
[11] C. S. Peskin, "Self-synchronization of the cardiac pacemaker. Mathematical Aspects of Heart Physiology", New York University: New York, **(1975)**, pp. 268-278.
[12] M. Maroti, B. Kusy, G. Simon and A. Ledeczi, "The flooding time synchronization protocol", Proceeding ACM SenSys '04, San Diego, **(2004)**.
[13] H. Song, S. Zhu and G. Cao, "Attack-resilient time synchronization for wireless sensor networks", IEEE Transactions on Computers, vol. 25, no. 1, **(2005)**, pp. 765-772.
[14] R. M. Anderson and R. M. May, "Infectious Diseases of Human: Dynamics and Control", Oxford: Oxford Univ. Press, **(1991)**.
[15] J. L. Sanders, "Quantitative guidelines for communicable disease control programs", Biometrics, vol. 27, **(1971)**, pp. 883-893.
[16] H. W. Hethcote, "An immunization model for a heterogeneous population", Theoretical population biology, vol. 14, no. 12. **(1978)**, pp. 338-349.
[17] P. De, Y. Liu and S. K. Das, "An epidemic theoretic framework for evaluating broadcast protocols in wireless sensor networks", Proceeding of IEEE International Conference on Mobile Ad-hoc and Sensor Systems, Pisa, **(2007)**.

Author

Zhiling Tang, he received the B.S. and M.S. degree in communications engineering from Guilin University of Electronic Technology, China, in 1997 and 2005, the Ph.D. degrees in information and communications engineering from Xidian University, China, in 2013. Now he is an associate professor in Guilin University of Electronic Technology, China. His main research interests include next generation of wireless sensor networks.