doi:10.3772/j.issn.1006-6748.2015.02.004

Clustered trajectories anonymity in wireless sensor networks①

Seble Hailu Dady, Wang Jiahao②, Qin Zhiguang, Yang Fan
(School of Computer Science & Engineering, University of Electronic Science and Technology of China, Chengdu 611731, P.R.China)

Abstract

This paper proposes a clustered trajectories anonymity scheme (CTA) that enhances the k-anonymity scheme to provide the intended level of source location privacy in mobile event monitoring when a global attacker is assumed. CTA applies isomorphic property of rotation to create traces of the fake sources distributions which are similar to those of the real sources. Thus anonymity of each trajectory and that of the clustered is achieved. In addition, location k-diversity is achieved by distributing fake sources around the base station. To reduce the time delay, tree rooted at the base station is constructed to overlap part of the beacon interval of the nodes in the hierarchy. Both the analytical analysis and the simulation results prove that our scheme provides perfect anonymity with improved energy overhead and time delay.

Key words: clustered trajectories anonymity scheme (CTA), source location privacy, k-anonymity, global attackers, wireless sensor networks (WSNs)

0 Introduction

Recently wireless sensor networks (WSNs) are extending their applications into many areas such as health care, environmental monitoring and wild life monitoring. In these application areas source location privacy providing is critical. This is because the exposure of the location of the source node leads to the location of the sensitive object under supervision. But source location privacy providing is a challenging task especially when the attacker is a global attacker and the monitored objects are mobile. One reason is that the spatio-temporal data associated with the mobile object is rich in correlation information.

Solutions proposed to provide source location privacy against global attacker[1,2] introduce excessive energy overhead due to network wide dummy message injection. To trade off privacy with communication cost and latency, Mehta, et al.[1] proposed source simulation. In source simulation few sensor nodes are randomly selected to simulate the mobility of the monitored object. But building and implementing the object's mobility profile is still an open research topic[1]. Scheme proposed in Ref.[3] switch statistically strong source anonymity (SSSA) scheme in Ref.[2] to a k-anonymity scheme in Ref.[1] on demand, but mobile event monitoring which can create real trajectory is not considered. Trajectory anonymity is addressed in a distributed manner in Ref.[4] but the solution applies only for events that start at the perimeter of the network and end somewhere inside the network.

Spatio-temporal data expose not only the movement pattern of each monitored object but also the relationship between different monitored objects and their interaction with the environment. One aspect of this is hotspot. As discussed in Ref.[5] hotspot phenomenon causes an obvious inconsistency in the network traffic pattern. This is because a large volume of packets are originating from a small area. Thus, analysis of traffic may also lead to a cluster of trajectories that expose the mobility patterns of a collection of monitored objects.

This paper considers WSNs deployed for wild life monitoring that demand privacy but tolerate time delay in the order of few seconds. Based on this application, but not limited to it, a clustered trajectories anonymity scheme (CTA) is proposed. This scheme provides anonymity to all possible correlation information that can be deduced from the spatio-temporal data associated with event reporting such as trajectory made by monitored object or cluster of trajectories made by the collection of monitored objects. In addition, location k-diversity is achieved by selecting fake sources distributed around the base station (BS). Our scheme also satisfies that fake sources should be comparable to the real

① Supported by the National Natural Science Foundation of China (No. 60903157), the Fundamental Research funds for the Central Universities of China (No. ZYGX2011J066) and the Sichuan Science and Technology Support Project (No. 2013GZ0022).

② To whom correspondence should be addressed. E-mail: wangjh@uestc.edu.cn

Received on Feb. 5, 2014

source with respect to their distances to the BS[6]. To achieve all these there is no need to know the mobility pattern and movement speed of the monitored objects as in Refs [1,4]. Instead our scheme applies isomorphic property of rotation at BS to select fake sources. To reduce energy cost dummy messages are on demand and the beacon frames at MAC layer are used to send event notification message to the BS. Time delay during event notification is reduced by constructing tree rooted at BS to overlap part of the beacon intervals of nodes in the hierarchy. The analytical analysis and the simulation results show that our scheme provides perfect source location anonymity with improved energy cost and time delay.

1 Related work

Several protocols to provide source location privacy have been proposed[1-7], but a solution that guarantees efficient privacy against global attackers remains hard to pin down. The threat of global adversaries is first considered by Mehta et al.[1]. The authors proposed the periodic collection and source simulation schemes. Periodic collection scheme provides maximum location privacy but the network wide dummy messages consume significant amount of sensor energy while increasing the network collisions and decreasing the packet delivery ratio. Shao, et al.[7] proposed a scheme which conveyed data to the base station only using beacon frames at the MAC layer. Since beacons are periodically broadcasted regardless of the occurrence of real events, this approach provides perfect event source unobservability at no additional energy cost. However, since the time between consecutive beacons is relatively large, the solution is impractical for nodes that have successive messages to send.

Mehta, et al.[1] proposed a second technique called source simulation which aimed at trading off energy consumption with privacy. In this scheme the real event is hidden among $k-1$ fixed fake events simulating the mobility patterns of the monitored object. But randomly selecting the nodes that simulate the movement patterns of the monitored object and the constant number of fake events may leak correlation information when multiple objects are monitored. Also in applications that monitor heterogeneous objects there is a need to implement multiple models to the sensor nodes which increases complication and overhead. The solution proposed in Ref. [3] randomly selects fake sources when it switches from SSSA to k-anonymity scheme, but trajectory anonymity is not considered. The advanced form of k-anonymity scheme called l-diversity is proposed in Ref. [3]. L-diversity is used in this scheme to diversify location of fake sources in order to decrease the attacker information gain when he tries to search the object in the suspected areas. Unobservable handoff trajectory protocol is proposed in Ref. [4] to hide trajectory of events that may change frequently in a distributed environment. Even if this scheme provides solution to handoff problem for the events with the assumed movement speed, it does not provide privacy for events that start inside the network such as wild life monitoring.

2 Problem formulation

2.1 Network model

Beacon-enabled IEEE 802.15.4 is proposed used in wireless sensor network platforms such as ZigBee[8] to announce node presence and exchange system parameters. Beacon interval ranges from 15.36 milliseconds to 786.432 seconds as defined in IEEE 802.15.4. The considered WSN consists of the BS and a large number of homogenous sensor nodes which are randomly deployed in an area of interest as illustrated in Fig. 1. The sensor nodes are resource constrained devices with low battery power and computation capacity but equipped with sensing, data processing, and communicating components. A BS connecting to the outside infrastructure such as the Internet collects data from the network. We assume it is located at the centre of the deployment area and is resourceful. Each sensor node is assumed to know its location with Global Positioning System (GPS) or other mechanisms mentioned in Ref. [9] and share this information with the neighbouring nodes and the BS. Message between sensor node and the BS is communicated by using encryption techniques. Although key management and the packet content confidentiality are beyond the scope of this paper, we recommend[10] it for further reading.

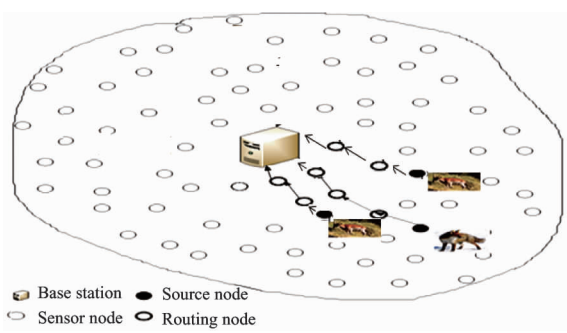

Fig. 1 The architecture of the considered network

2.2 Attacker model

A global attacker that is assumed in this work can eavesdrop every packet transmission in the network,

examine the encrypted packets, analyze network-wide traffic, determine traffic density on every link in the wireless sensor network and search the place where he suspects the object. However, the attacker cannot inject, modify or interrupt packet transmissions and can neither decrypt the content of captured packets.

2.3 Problem definition

Conventional k-anonymity schemes randomly select fake sources to provide source location privacy against global attackers. But these schemes have limitations to provide anonymity to trajectories and other correlation information from traffic analysis of spatio-temporal data collected when mobile objects are monitored. Traffic information collected from a WSN for a discrete time interval $\{t_1, t_2, \cdots, t_n\}$ includes tuples (x_1, y_1, t_1), (x_2, y_2, t_2), $\cdots$, (x_n, y_n, t_n) where (x_i, y_i) is the location of a node that reports event occurrence and t_i is the event reporting time. Analysis of these might provide the trajectory made by the monitored object defined as:

$T_i = \{(x_1, y_1, t_1), (x_2, y_2, t_2), \cdots, (x_k, y_k, t_k)\}$, where $(t_1 < t_2 < \cdots < t_k)$. Based on this, trajectory similarity is defined as follows:

Definition 1 (Trajectory Similarity): Two trajectories T_i and T_j are said to be similar if:

i. for any tuple $(x_k, y_k, t_k) \in T_i$, $\exists (x_h, y_h, t_k) \in T_j$ and

ii. for any (x_k, y_k, t_k), $(x_{k+1}, y_{k+1}, t_{k+1}) \in T_i$ and (x_h, y_h, t_k), $(x_{h+1}, y_{h+1}, t_{k+1}) \in T_j$, it holds that $\| (x_k, y_k), (x_{k+1}, y_{k+1}) \| \approx \| (x_h, y_h), (x_{h+1}, y_{h+1}) \|$

This implies that two trajectories are similar if they are defined in the same time interval and distances travelled by the two trajectories are almost the same at each time interval.

For a WSN applied to monitor a collection of objects, trajectory anonymity of each object to be monitored may not be enough. Because collection of trajectories can also provide correlation information such as hot spot created by group movement of the monitored objects or nature of objects to visit the same place for some purposes. Thus, distribution of the monitored objects in the monitored area needs also anonymity. This distribution is defined as cluster of trajectories.

Definition 2 (Clustered Trajectories Similarity): A collection of trajectories $T_C = \{T_0, T_1, \cdots, T_n\}$ and $T_F = \{T_{f0}, T_{f1}, \cdots, T_{fn}\}$ are similar if

i. $\forall T_i \in T_C$, $\exists T_{fk} \in T_F$ such that T_i and T_{fk} satisfy trajectory similarity and

ii. $\forall T_h, T_i \in T_C$, $\exists T_{fk} T_{fl} \in T_F$ such that **Dist** $(T_h, T_i) \approx$ **Dist** (T_{fk}, T_{fl}) at all corresponding points.

Hence clustered trajectories similarity implies trajectory similarity and collection of trajectories location relationship anonymity in terms of distance between trajectories. If the real trajectories are collected in one place, the same thing will happen for fake trajectories.

Definition 3 (Clustered Trajectories k-anonymity): A cluster of real object trajectories T_c is k-anonymous if there are $k - l$ clusters of fake trajectories $T_{F1}, T_{F2}, \cdots, T_{F(k-1)}$ that are similar to T_c.

This implies clustered trajectories k-anonymity also satisfies trajectory k-anonymity. Because $\forall T_i \in T_c$, $\exists T_{fj} \in T_{Fj}$ where $j = 1, 2, \cdots, k-1$ such that T_i is similar to T_{fj}.

For an attacker that performs an onsite examination distributing the suspected nodes affects his cost of finding the source node[3]. Based on this l-diversity[3] is adopted to WSNs in order to improve location diversity of the fake sources. The idea is that suppose the network area is divided into $L(L > 0)$ partitions of almost the same size. For the total number N of the sensor nodes in the WSN, assume S denotes a set of nodes where $S \subseteq N$ and $P(S)$ denotes the total number of different partitions that nodes in S are from. If $P(S) \geqslant l$ for $0 < l \leqslant L$ then l-diversity is achieved. Based on this, it is defined that spatial k-diversity is as follows:

Definition 4 (Spatial k-diversity): A set of nodes $S \subseteq N$ has a property of spatial k-diversity if $P(S) = L = k$.

The other problem in the k-anonymity scheme is that dummy traffics are on demand for reducing energy cost. This in turn needs a message to initiate communication. In the presence of global attackers, initiating communication without scarifying anonymity, energy overhead and time delay is a challenging issue. Previous researches have only partially addressed all problems mentioned above. This has motivated us to design clustered trajectories anonymity scheme (CTA).

3 Clustered trajectories anonymity scheme (CTA)

In this section three phases of CTA scheme are described bootstrapping (beacon interval) phase, fake source location calculation phase, and fake source assignment and message transfer phase.

3.1 Beacon interval

To trade off privacy with energy efficiency, the best method is reducing the number of fake sources and initiating fake message only when there is an event to

report. To make fake message generation on demand we use the beacon frame at MAC layer in beacon enabled WSN. In CTA the source node inserts event notification message that contains event id, timestamp, event location and number of messages to be sent in the beacon payload.

In beacon enabled WSNs every node in the network has independent beacon interval and sends the beacon message at the end of this interval. This introduces cumulative delay in sending event notification to the BS. To reduce time delay we use hierarchical routing which is common in WSNs[11]. A tree rooted at the BS is constructed as shown in Fig. 2. The purpose of this tree is to overlap the delay of the beacon messages for nodes in the hierarchy.

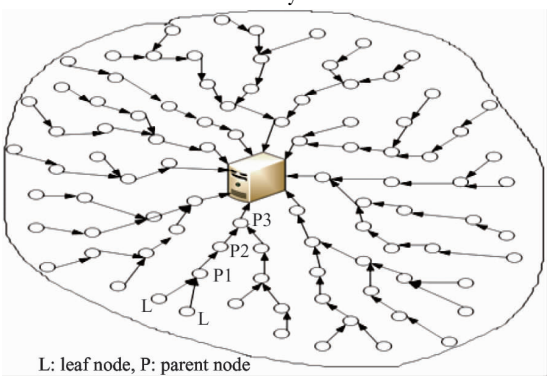

Fig. 2 Hierarchical transfer of beacon messages

A leaf node sends beacon messages to the parent node at the end of the beacon interval. The parent node initiates a beacon message when it accepts beacon message from the child node. The parent node decrypts and processes the accepted beacon message and sends it to its parent node without additional delay. This will continue until the beacon message reaches to the BS. Thus the beacon interval for each node starts from the time it sends a beacon message until the next beacon message arrives to it which also includes part of the delay at the leaf node. To do this the BS needs only to identify the leaf nodes and assign interval on these nodes. These nodes initiate beacon messages based on their interval.

As illustrated in Fig. 3, the beacon interval starts at t_0. Leaf node L sends its beacon massage at t_1 which is the end of the first beacon interval. Parent P_1 sends the beacon message only by taking time to process beacon from L, parent P_2 do the same after accepting the beacon from P_1 and finally P_2 sends the beacon to the BS. The process will continue with this pattern for all time intervals t_1, $t_2\cdots$. Thus the average time delay for event notification message that is hidden in the beacon frame to reach the BS is $t_d/2$ where t_d is the beacon interval. The BS calculates fake sources locations and initiates message communication at the end of each beacon interval.

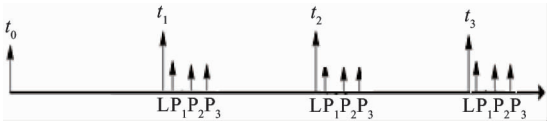

Fig. 3 Beacon interval overlaps

3.2 Fake source location calculation

Traffic collected from WSN deployed to monitor mobile objects exposes correlation information such as the trajectory made by the monitored object and how monitored objects are distributed in the network area which may in turn lead to the current source node location. To provide real event report distribution we use isomorphism which is studied in mathematics in order to extend insights from one phenomenon to others. If two objects are isomorphic, then any property which is preserved by an isomorphism and which is true of one of the objects is also true of the other.

The distance between the nodes that report event occurrences are the main sources of correlation information for an adversary. One example of isometric functions that preserve distance is rotation. The point (x, y) is rotated by angle β to find (x', y') using the following formula:

$$x' = x\cos\beta - y\sin\beta,\ y' = x\sin\beta + y\cos\beta$$

Generally rotation about a fixed point preserves distance and angle. This advantage is taken to create $k-1$ sets of fake reports; each set will have distances between fake sources similar to the distances between sources that report real event occurrences. Every time when the source sends event notification to BS, BS calculates the fake sources locations by rotating the source node location by angles β, $2\beta,\cdots,(k-1)\beta$. In our case β is calculated as $\beta = 360/\mathrm{k}$ to diversify the k nodes around the BS. Algorithm 1 describes the details of how the BS calculates fake source locations from the real source location.

Algorithm 1: Fake source location calculation.

Input: source location (x_0, y_0), number of fake sources plus the real source k
Output: location of the $k-1$ fake sources
Procedure:
1. $\beta = 360/\mathrm{k}$
2. for $i = 1$ to $k-1$ do
3. $x_i = x_0\cos(i\times\beta) - y_0\sin(i\times\beta)$
4. $y_i = x_0\sin(i\times\beta) + y_0\cos(i\times\beta)$
5. $f_i = (x_i, y_i)$
6. end for
7. return $f_1, f_2, \cdots, f_{k-1}$

From Fig. 4 for $k = 4$ fake sources F1, F2 and F3 are located by rotating real source location R by an angle $\beta = 360/4 = 90^0$, 180^0, and 270^0. When the new source location is R' the new fake sources are located by the same calculation but by the coordinate of R'. Thus the distance RR' is maintained by the fake sources distances F1F1', F2F2' and F3F3'.

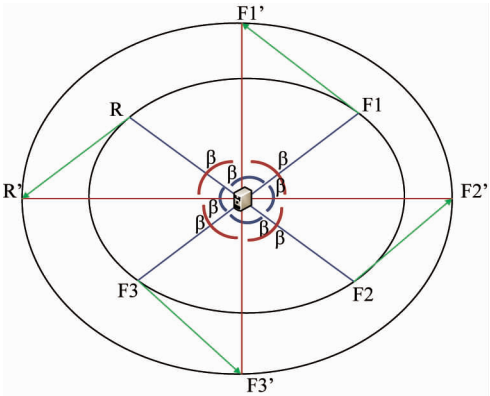

Fig. 4 Locating fake sources around the BS

3.3 Fake sources assignment and message transfer

Calculating location of fake sources based on Algorithm 1 provides ideal location. That is, there may not be a sensor node at the calculated location. In this case BS selects nodes that are closer to the calculated points as fake sources, and then it broadcasts the fake sources assignment message by introducing the real source location. Following this the fake and real sources start to generate messages at the same pattern. In the case when BS accepts event notification from a large number of source nodes, it schedules the fake assignment or drops the old event notification message if more than one source node detects the same event. This contributes to the reduction of energy consumption.

3.4 Discussion

Random location of BS: for BS located randomly in WSN we can apply translation instead of rotation to select fake sources which also has isomorphic property to preserve distance.

Non-beacon enabled WSNs: In this type of WSN it is possible to make every node to generate fake event notification messages at the beacon interval to provide unobservablity to the source with real event notification. To minimize energy cost, message size at this interval can be smaller than the size of the event reporting message in this interval.

4 Analysis of the scheme

4.1 Analytical analysis

4.1.1 Privacy analysis

Theorem 1: CTA satisfies clustered trajectories k-anonymity property.

Proof: To prove that CTA satisfies clustered trajectories k-anonymity, first we have to show that CTA satisfies trajectory similarity and $T_i = \{(x_0, y_0, t_0), (x_1, y_1, t_1), \cdots, (x_n, y_n, t_n)\}$ is a real trajectory of the monitored object analyzed from the traffic collected at discrete time intervals $\{t_0, t_1, \cdots, t_n\}$ where $(t_1 < t_2 < \cdots < t_n)$. In CTA, before a source node starts to report real event occurrence, BS calculates and assigns $k - 1$ fake sources that report at the same pattern and time with the real source. Thus $\forall (x_i, y_i, t_i) \in T_i$, $\exists (x_i \cos(j \times \beta) - y_i \sin(j \times \beta), x_i \sin(j \times \beta) + y_i \cos(j \times \beta) t_i) \in T_j$ for $1 \leqslant j < k$. This implies T_j contains a collection of points that are defined at the same time interval with points in T_i.

To show the distance travelled by the fake trajectory (D') at any point is the same as the real trajectory distance (D), suppose (x_i, y_i) and (x_j, y_j) are random locations of nodes that report real event occurrences at time t_i and t_j, distance D between (x_i, y_i) and (x_j, y_j) is

$$D = \sqrt{(y_i - y_j)^2 + (x_i - x_j)^2} \tag{1}$$

Distance D' after rotation of (x_i, y_i) and (x_j, y_j) at an angle $j \times \beta$ where $0 < j \times \beta < 2\pi$ is:

$$\begin{aligned} D' &= \sqrt{(x_i \sin j \times \beta + y_i \cos j \times \beta - x_j \sin j \times \beta - y_j \cos j \times \beta)^2 + (x_i \cos j \times \beta - y_i \sin j \times \beta - x_j \cos j \times \beta + y_j \sin j \times \beta)^2} \\ &= \sqrt{[(y_i - y_j)^2 (\cos^2 j \times \beta + \sin^2 j \times \beta) + (x_i - x_j)^2 (\cos^2 j \times \beta + \sin^2 j \times \beta)]} \\ &= \sqrt{(y_i - y_j)^2 + (x_i - x_j)^2} \end{aligned}$$

This implies $D = D'$ when there is a deviation of the actual fake source location from the calculated

$$D \approx D' \tag{2}$$

Because of the dense deployment of WSN, this deviation is insignificant to differentiate the fake trajectory from the real one. Thus from Eqs(1,2) CTA satisfies trajectory similarity. And since a single source node location is rotated by angles β, $2\beta, \cdots$, $(k - 1)\beta$, $K - 1$ fake trajectories exist for each real trajectory, which implies CTA satisfies trajectory k-anonymity. Also for each real trajectory in trajectory set $\{T_0, T_1, \cdots, T_n\}$ which are analyzed from the traffic collected, it is possible to find $k - 1$ collections of fake trajectories. When we categorize the fake trajectories by the angles of rotation we will find $k - 1$ cluster of trajectories $\{C_1, C_2, \cdots, C_{k-1}\}$. C_1 contains a cluster of trajectories found by rotating points in T_0, T_1, $\cdots$, T_n by an angle β, C_2 by an angle $2\beta, \cdots$ and C_{k-1} by an angle $(k - 1)\beta$. Thus $\forall T_h$, $T_i \in \{T_0, T_1, \cdots, T_n\}$, $\exists T_{jl}$, $T_{kl} \in C_l$ where $l = 1, 2, \cdots, k - 1$ such that **Dist** $(T_h, T_i) \approx$

Dist (T_{jl}, T_{kl}). Therefore it is concluded that CTA satisfies clustered trajectories k-anonymity.

Theorem 2: CTA satisfies the property of location k-diversity.

Proof: Dividing the network area into equal parts with BS as a centre is similar to dividing the circle into equal parts. When point on the perimeter of the circle are divided into k equal parts, they are always the points that are $360^0/k$ apart are from different sections of the circle. Since CTA uses angles β, $2\beta\cdots(k-1)\beta$ to rotate the source location, consecutive fake sources are approximately $\beta = 360^0/k$ angle far apart around the BS. Thus all the k points are almost from k different sections of the network. Therefore CTA satisfies location k-diversity.

4.1.2 Time delay analysis

The time delay of CTA for sending messages is the same with that of the dynamic source anonymity after the fake sources are selected. However when the time it takes to send an event occurrence message to BS for fake source request, each node has its independent beacon interval: $t = (t_d/2 + t_s)h$, where h is the maximum number of hops from the BS, t_s is the time to send event notification message and $t_d/2$ is the average time delay of a beacon message on each node that participates in forwarding the beacon message. But in CTA, beacon intervals overlap so that $t = t_d/2$ which is independent of h and t_s. In case of dynamic source anonymity the time delay for sending fake request is $t = (t_s + t_{sd})h + t_w$, where t_{sd} is the shortest on each sensor node, h is the number of hops from source to the BS and t_w is the waiting time at BS before it broadcasts the fake source assignment message.

4.1.3 Energy overhead

The energy overhead for dynamic source anonymity scheme when a single source node reports event related information is: $E_T = E_d + knE_m$, where E_d is the average energy cost of sending event notification message, k is the total number of nodes that participate in sending messages at the same time interval, n is the total number of messages sent by each node, and E_m is the average cost of sending a single message from source to BS. But since beacon messages have no energy overhead for CTA, $E_T = knE_m$.

4.2 Simulation results

A discrete simulator has been built up to evaluate the performance and security of our scheme using TinyOS. 1,000 sensor nodes are randomly deployed in a round area network with a diameter of 50. The transmission range is set to 1. The base station is located at the centre of the network. The network has one hot spot that is randomly located and fixed during each simulation run to show the hot spot created due to different objects that visit the area from different directions. In our simulation 10 objects visit the hot spot area repeatedly.

4.2.1 Privacy analysis

The false positive hot spot detection ratio of the attacker is compared when random selection and CTA scheme are applied. The attacker first performs rate monitoring to detect the most visited area and then studies the trajectory around the detected hot spot area to determine whether it is the real hot spot area or a fake one. In random selection, fake sources may or may not form the hot spot areas as randomly selecting fake sources which are distributed throughout the network. Even when fake sources form hot spots by chance there may not form a pattern of movement that resemble the real event movement around the hot spot. But in case of CTA isomorphic property of rotation copies any pattern observed by the real event report on fake reports.

As it can be seen from Fig. 5, when the number of traffic collected for analysis increases, the probability of detecting false hot spots increases. This is because hot spot is created when there is large volume of data in the network. When we compare the false positive hot spot detection ratio of our scheme with random selection, our scheme gives 90% of the time hot spot that is false positive for $k = 10$. This is because there are exactly 9 false hot spots for a single hot spot which provides exact k-anonymity. But random selection of fake sources ends up in 50 % probability of detecting false

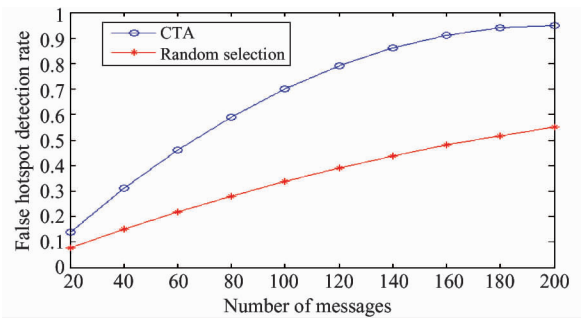

Fig. 5 False positive hot spot detection ratio for $k = 10$

positive hot spot. Generaly, when we see the number of hot spots detected for different values of k, in the proposed scheme k hot spots are detected as we can see from Fig. 6, which implies the probability of detecting the real hot spot is $1/k$. But the number of hot spots detected in random selection is always less than k as indicated in Fig. 6 and hence there is a chance to detect the real hot spot only.

4.2.2 Time delay

We compare the time delay for sending event notification in the case of Dynamic SSSA , CTA without

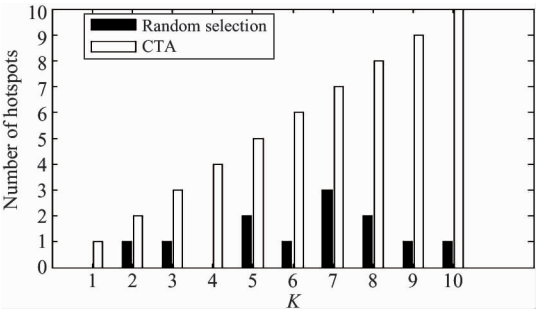

Fig. 6 Hot spots detected for different values of k

beacon interval overlaps, and CTA. Dynamic SSSA has less time delay when there is less frequent fake request from the source node. But when the number of fake requests increases, the attacker may detect a consecutive short time delay which in turn implies that there are real event notifications. Thus, time delay increases for providing source location privacy. CTA without beacon interval overlap has a large time delay because each node has independent beacon interval and consequently cumulative delay is introduced for the event notification to arrive at BS. But the time delay decreases with significant amount when the beacon intervals overlap as we can see from Fig. 7.

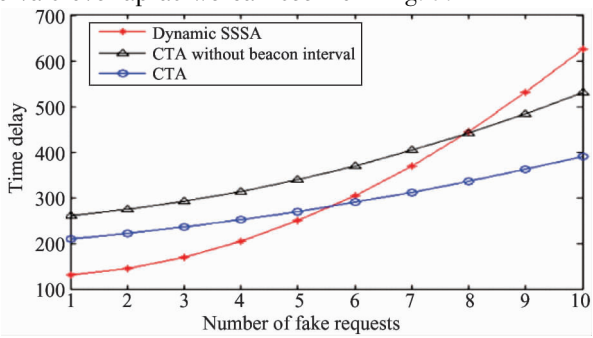

Fig. 7 Time delay comparison

4.2.3 Energy consumption

To send the same amount of message within a given time T, SSSA consumes more energy due to network wise dummy message injection. Dynamic SSSA reduces the energy cost by extending the delay of network wise dummy message injection. CTA consumes the least energy as fake request is sent within the beacon frames at MAC layer which have no energy overhead. Fig. 8 shows this clearly.

5 Conclusion

This study proposes a scheme that provides perfect k-anonymity to the source that reports event occurrence in mobile events monitoring application against a global attacker. The analytical analysis and the simulation results show that our scheme is efficient and effective in providing the desired anonymity.

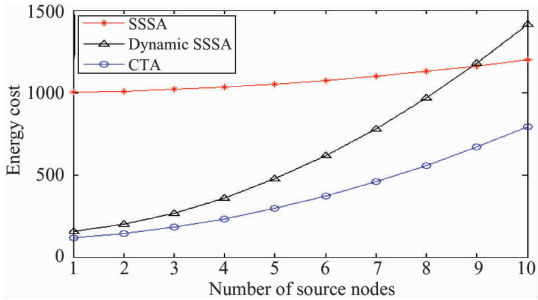

Fig. 8 Energy overhead

References

[1] Mehta K, Liu D, Wright M. Location privacy in sensor networks against a global eavesdropper. In: Proceedings of the IEEE International Conference on Network Protocols, Beijing, China, 2007. 314-323

[2] Shao M, Yang Y, Zhu S C, et al. Towards statistically strong source anonymity for sensor networks. In: Proceedings of the 27th IEEE Communications Society Conference on Computer Communications, Phoenix, USA, 2008. 466-474

[3] Yang Y, Zhu S C, Cao G H, et al. An active global attack model for sensor source location privacy: analysis and countermeasures. *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering*, 2009, 19:373-393

[4] Ortolani S, Conti M, Crispo B, et al. Events privacy in WSNs: A new model and its application. In: Proceedings of the IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks, Lucca, Italy, 2011. 1-9

[5] Mahmoud M, Shen X M. A cloud-based scheme for protecting source-location privacy against hotspot-locating attack in wireless sensor Networks. *IEEE Transactions on Parallel and Distributed Systems*, 2012, 23(10):1805-1818

[6] Kamat P, Zhang Y Y, Trappe W, et al. Enhancing source-location privacy in sensor network routing. In: Proceedings of the 25th IEEE international Conference on Distributed Computing Systems, Columbus, USA, 2005. 599-608

[7] Shao M, Hu W H, Zhu S C, et al. Cross-layer enhanced source location privacy in sensor networks. In: Proceedings of the 6th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, Rome, Italy, 2009. 1-9

[8] Li Z. ZigBee wireless sensor network in industrial applications. In: Proceedings of the 2006 SICE-ICASE International Joint Conference, Busan, Korea, 2006. 1067-1070

[9] Avinash K, Sonu A. Location detection in wireless sensor network using classical optimization methodology. *International Journal of Computer Science and Technology*, 2012, 3(1):685-688

[10] Zhao J. Research on key predistribution scheme of wireless sensor networks. In: Proceedings of the 5th International Conference on Intelligent Computation Technology and Automation, Zhangjiajie, China, 2012. 287-290

[11] Iwanicki K, Van S M. On hierarchical routing in wireless sensor networks. In: Proceedings of the International Conference on Information Processing in Sensor Networks, San Francisco, USA, 2009. 133-144

Seble Hailu Dady, born in 1976. She is Ph. D student in University of Electronic Science and Technology of China. She received B. Ed in Mathematics from Haramay University in 2000, B. Sc and M. S degree in Computer Science from Addis Ababa University in 2004 and 2008 respectively. Her research interest mainly focuses on privacy and security in wireless sensor networks and related applications.