Data analysis of simulated WoT-based anti-crime scenario

Chih-Chi Kuang

Department of Business Administration,
National Taipei University,
San Shia District, New Taipei City, 23741, Taiwan
Email: s810431101@webmail.ntpu.edu.tw

Kuei Min Wang

Department of Information Management,
Shih Chien University,
University Road, Neimen., Kaohsiung, 84550, Taiwan
Email: willymarkov0413@gmail.com

Lin Hui*

Department of Innovative Information and Technology,
Tamkang University,
Linwei Rd., Jiaoxi Township, Yilan County 26247, Taiwan
Email: 121678@mail.tku.edu.tw
*Corresponding author

Chuan-Yu Chang

Department of Computer Science and Information Engineering,
National Yunlin University of Science and Technology,
University Road, Douliou, Yunlin 64002, Taiwan
Email: chuanyu@yuntech.edu.tw

Kuang Hui Chiu

Department of Business Administration,
National Taipei University,
San Shia District, New Taipei City, 23741, Taiwan
Email: khchiu@mail.ntpu.edu.tw

Abstract: This study proposes a novel WoT concept for improving the current police work on anti-terrorist. In order to prove the feasibility and effectiveness, the presented WoT-based police rescue squad force (RSF) concept is modelled and simulated by a Monte Carlo simulation. The current RSF and WoT-based are two alternatives that are analysed for the comparison. The simulation results show that a significant difference between the current RSF and WoT-based exists. The information gained from the simulation reveals the WoT-based RSF can support the commander's decision makers in performing the anti-terrorist task with less risk, less cost with high effectiveness. This study makes an exceedingly contribution which the WoT-based RSF concept is viable and can easily improve police performance in anti-terrorist and hostage rescue tasks.

Keywords: wireless sensor network; WoT; internet of things; IoT; rescue squad force; RSF; simulation; terrorist; unmanned aerial vehicle; UAV.

Reference to this paper should be made as follows: Kuang, C-C., Wang, K.M., Hui, L., Chang, C-Y. and Chiu, K.H. (2021) 'Data analysis of simulated WoT-based anti-crime scenario', *Int. J. Web and Grid Services*, Vol. 17, No. 1, pp.3–19.

Biographical notes: Chih-Chi Kuang is a PhD student at Department of Business Administration, National Taipei University, Taiwan. She holds a Master's degree in Public Administration and Policy from National Taipei University in 2008. Her current interest in academic is the strategical analysis, information management and decision support system.

Kuei Min Wang received his Master's degree of Operations Research at Naval Postgraduate School in Monterey, California and PhD degree in Information Engineering from the University of Tamkang, Taipei, Taiwan. He was a Senior Analyst in Strategy and Resource Allocation in Government. He is an Associate Professor in Information Management Department at Shih-Chien University for teaching operations research, decision support system, simulation and quantitative techniques. His research has been heavily on data analytics, decision support with internet of things (IoT), innovative concept feasibility study and the system analysis of effectiveness and performance.

Lin Hui is an Associate Professor of the Department of Innovation Information and Technology at Tamkang Universit, Taiwan, ROC. She received her BS degree in Mathematics from Tunghai University and MS degree in Mathematics from Fu Jen Catholic University, Taiwan. In 1993, she got the support from the Chungshan Institute of Science to be a special student in the Department of Computer Science at the University of Wisconsin-Madison, USA. She received her PhD degree in Computer Science and Information Engineering from Tamkang University, Taiwan, in 2006. Her current research interests include operation research, data mining and multimedia applications.

Chuan-Yu Chang received his BS and MS degrees in Navigation Science and Electrical Engineering from National Taiwan Ocean University, Taiwan, in 1993 and 1995, respectively, and PhD degree in Electrical Engineering from National Cheng Kung University, Taiwan, in 2000. He is currently a Full Professor of the Department of Computer Science and Information Engineering, National Yunlin University of Science and Technology, Taiwan. He is an Associate Editor of the *International Journal of Control Theory and Applications*. His current research interests include neural networks and their application to medical image processing, wafer defect inspection, digital watermarking and pattern recognition.

Kuang Hui Chiu is a Professor in the Department of Business Administration, National Taipei University, Taiwan. He received his PhD degree of Management Decision in Computer from Tsing Hua University in Taiwan in 1985. His current academic interests include information management, management program design, data structure, e-commerce and database management.

1 Introduction

Hostages held by terrorists have been a serious issue for governments and has a great impact on society as it takes many social resources and time to resolve. Due to the low cost and ease of use, the concept of the web of things (WoT) can be applied in police work to help minimise the time, manpower, and risk involved in performing such tasks. Techopedia (2012) defined the WoT as "a 'things' to have embedded computer systems that enable communication with the Web. Such smart devices would then be able to communicate with each other using existing Web standards".

The sensors connected to the internet make ad hoc connections, share data and allow unexpected applications to form the IoT, much like the human nervous system (Ashton, 2017). With a sharp weapon such as IoT, humans can rely on it to build new applications in a range of areas, such as business, industry, government, healthcare, etc. (Kusek, 2018). However, Atzoria et al. (2017) pointed out that the heterogeneity of the IoT includes both hardware and software. The hardware in the IoT includes integrated devices from multiple vendors. The software run on devices uses multiple internet and data exchange formats. The current scenario of IoT is therefore that devices/things are not fully interoperable. In order to facilitate communication between the devices and integrate them into system of systems, a common communication interface is required.

Key to the hostage rescue task is the situation awareness that can be built by a wireless sensor network (WSN) linked to the internet. Some of the sensors are carried by an unmanned aerial vehicle (UAV) or an unmanned ground system (UGS), which are mainly used in search and detection assignments. This paper proposes a way of examining the effectiveness of using the WoT to support the police rescue squad force (RSF) as it crosses the screens set up by terrorists to counter the police as they try to rescue hostages. A specific scenario was developed, and models with Monte Carlo simulation were created and the results analyzed. The data clearly indicate the effectiveness of the WoT applied to the current scenario. Several cases were generated to compare the effectiveness of the conventional and the WoT-based RSF. However, it was difficult to distinguish a significant difference between cases by the output data, so statistical techniques were adopted to perform further analyses in order to define the significance level of the difference.

2 Literature review

According to Roser et al. (2018), between 1970 and 2016, there were 511,047 terrorist incidents worldwide, resulting in 1,150,580 deaths. Miller (2016) stated that in 2016 terrorist attacks took place in 104 countries, with 55% in five countries (Iraq, Afghanistan, India, Pakistan, and the Philippines), and 75% of all deaths due to terrorist attacks taking place in five countries (Iraq, Afghanistan, Syria, Nigeria, and Pakistan). The Islamic State of Iraq and Syria (ISIS) were responsible for more attacks and deaths than any other perpetrator group in 2016. The counter terrorist (CT) special response force originated in Israel in 1957 for carrying out cross-border tactics against Palestinian guerrilla bases. Special Weapons and Tactics (SWAT) units emerged for managing hostage-taking incidents in the post-1972 era (Mahadevan, 2012).

There are many types of weapons and sensors that have been used by terrorist to hold hostage and fight against government forces. MacDonald and Lockwood (2003) indicate that landmines have claimed over 15,000 victims per year in some 90 countries. In order to clear these landmines, over a dozen methods have been developed and applied, such as electromagnetic induction, ground-penetration radar, X-ray backscatter, infrared/hyperspectral and acoustic/seismic, etc. However, these detection methods cannot guarantee a higher probability of detecting buried landmines. Other than RAND's proposed multi-sensor system to improve mine detection capability, several studies have also presented the efforts to decrease false alarms and so increase the probability of the detection of landmines (Núñez-Nieto et al., 2014). To detect an area with landmines in an emergency situation, manual processing would be relatively ineffective. A UAV carrying a specific light-weight sensor such as a metal detector, infrared camera, or custom-designed lightweight ground penetrating radar (GPR) to detect the landmines in the marked area would be fast and effective (Rajan et al., 2014). Cerquera et al. (2017) indicated that software defined radio (SDR)-based GPR in outdoor experiments has enabled the establishment of the following conditions and limits for an accurate detection: relative humidity > 70% (semi-wet or dry terrain), artefact depth 20 cm, and diameter (> 15 cm) with a transversal area > 16 cm^2 and > 30% of the material made of metal. In addition, the UGS, tele-operated ground vehicle, can also perform mine detection, mine clearing, and explosive ordnance disposal (Romanovs, 2016). For estimating the detection probability of any object moving within the security system detection area at any point in the detection range, Artyushenko et al. (2018) pointed out that normal and truncated normal distribution are required. Abdelwahab (2013) stated that the reported experiment could achieve close to 1.0 landmine detection probability by using SC-FDMA wireless.

Situation awareness is the key to keeping a war zone under control. The top priority of situation awareness is to be able to provide the identified location, deployment, and activity of the enemy, as well as friend force information. Situation awareness (SA) is one of the most critical factors in operation that can determine the mission accomplishment. There are many definitions of the term 'situation awareness', some of which are illustrated in the following. Endsley (1995a) suggested that SA provides "the primary basis for subsequent decision making and performance in the operation of complex, dynamic systems." At its lowest level, the operator needs to perceive relevant information (in the environment, system, self, etc.), then integrate the data in conjunction with the task goals, and at the highest level, predict future events and system states based on this understanding. Green et al. (1995) thought that SA requires an operator to "quickly detect, integrate and interpret data gathered from the environment. In many real-world conditions, situational awareness is hampered by two factors. First, the data may be spread throughout the visual field. Second, the data are frequently noisy." Wickens (1992) definition is simpler, "situation awareness refers to the ability to rapidly bring to consciousness those characteristics that evolve during a flight." However, the most frequently cited definition is by Endsley (2006), who defined it as: "the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and the projection of their status in the near future." Endsley also indicated that SA involves four levels of activities (Endsley, 1995b):

1 perceiving the status, attributes and dynamics of relevant elements in the environment

2 understanding the significance of those elements in light of the goals of the decision maker

3 projecting the future actions of the relevant elements and the consequences of these actions in that environment

4 sharing situational awareness, its components, and the decision-making process.

In order to achieve the goal of SA, it is necessary to rely on sensors to collect relevant data from the targeted field and to process the data in order to gain useful information for the local end-user. SA involves four levels of activities. Hence, from the design views in SA engineering, Kantorovitch et al. (2017) suggested that the SA system must support the end-user by providing an integrated view, supporting the work process, supporting decision-making, and being usable, simple and attractive. The common operating picture (COP) provides the end-user with an integrated view and is essential for creating SA. It is defined as a single identical display of relevant information shared by more than one command. A COP facilitates collaborative planning and assists all echelons to achieve situational awareness. It is the tool for a good level of SA. It is also regarded as an object of a structure or multipurpose repository hosting knowledge (United States Department of Defense, 2012; Timonen, 2018). The more essential issue in SA is the decision support in those inherent changing uncertainties in crisis and emergency scenarios. Colin Powell, former US Chairman of Joint Chief of Staff and Secretary of State, once said, "Tell me what you know, tell me what you don't know, tell me what you think, and make clear which is which." It needs to be so sure for the safety of a soldier. The premise is the soldier must catch a clear picture of the battlefield well enough. In order to achieve that, the gathered data from UAVs, ground sensors, and high altitude sensors need to be processed by analysis, data fusion, and synthesis, in order to transform them into meaningful information which can be shared and disseminated, or even to be interoperable by COP for action's decision support (Hodicky and Frantis, 2009; MacFarlane and Leigh, 2014).

The concept of the internet of things (IoT), such as the variety of sensors or sensor network, platforms, positioning devices, in the support of SA has been widely applied recently. The definition of IoT for smart environments by Gubbi et al. (2013) is "interconnection of sensing and actuating devices providing the ability to share information across platforms through a unified framework, developing a common operating picture for enabling innovative applications. This is achieved by seamless ubiquitous sensing, data analytics and information representation with cloud computing as the unifying framework." Other than sensors and actuators, the augmented reality (AR) can be a multiplier in the supporting end-users for providing important command control (C2) information of the environment that (You et al., 2018) indicated "accessing information via an AR system can elevate combatants' situational awareness to effectively improve the efficiency of decision-making and reduce the injuries." AR is defined as systems that have the following characteristics:

1 they combine real and virtual

2 they are interactive in real time

3 they are registered in 3-D.

AR can replace oral communication not only on head-mounted devices (HMDs) but by integrating the real and virtual objects in real time interactively into an individual's physical environment so that they can perceive the information existing in the surroundings (Mekni and Lemieux, 2014; Lukosch et al., 2015; Azuma, 19997). AR provides the user with superimposed information that can be seen in the real world, that is, it complements the real world with virtual information (Hicks et al., 2003).

The IoT is heterogeneous in terms of communication protocol and in data exchange formats. To resolve this problem, the WoT was developed to provide a common interface by translating the heterogeneity into homogeneity. The WoT (Guinard and Trif, 2009) employs the existing web protocols and technologies (e.g., HTTP, URL, web services) as the standardised way to access things in the physical world. The benefit of the WoT's WSN, according to Khan et al. (2017), is that it plays an important role in connecting objects to the IoT. In this study, the authors propose a WoT-based emerging sensor network (WoT-ESN) which collects data from sensors, routes sensor data to the web, and integrates smart things into the web by employing a representational state transfer (REST) architecture that makes a significant contribution to the smart home issue. In Wu et al. (2014), based on the WoT, the authors proposed the virtual environment of things (VEoT) to integrate real smart things with virtual avatars/objects for creating the virtual environment. They showed the effectiveness of WoT and VEoT.

Unmanned vehicles, including UAV and UGS, have an important role of carrying sensors and weapons to perform assigned missions. In light of technological advances, the UAV is an effective measure for the defensive side to monitor the potential threat. Sun et al. (2016) proposed an all-in-one camera-based target detection and positioning system for integrating into a fully autonomous fixed-wing UAV capable of on-board, real-time target identification, and post-target identification. However, lower altitude mini-UAV is easy to carry and deploy in the scenario of this study. Carrying the precision sensors, the UAV can loiter in the air for the purposes of detection of the ground target. Väärs (Romanovs, 2016) pointed out that the use of UAV has become an essential feature of land operations. This widespread technology is now systematically used by the militaries of almost all countries, and there has been an exponential increase in military investments in UAV. The specifications of the thermal camera include the sensor pointed out in Love (2017) with a resolution of 640 × 512, lens/FOV with 19 mm/32° × 26°, an operating temperature range from –21°C to + 50°C, a frame rate of 30 Hz, and an operational altitude of up to 3,048 m.

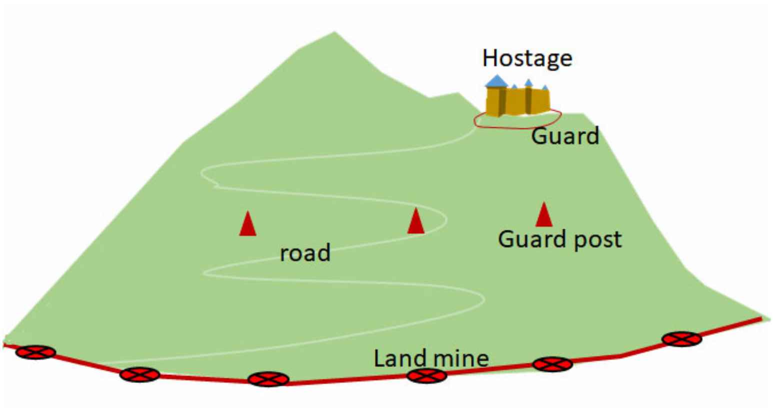
3 Model development

To model the hostage rescue mission for analytical purposes, we are concerned with three aspects of the mission: the scenario, operational concept, and algorithm.

Many different hostage rescue scenarios have occurred. However, to satisfy the analytical purpose of distinguishing the difference between the conventional and IoT-based rescue mission approaches, we intended to design a simple scenario for a simulation in order to identify the fundamental difference and to check if it is significant. The scenario consists of the two sides' interaction, i.e. the terrorist's defense and the police RSF's action.

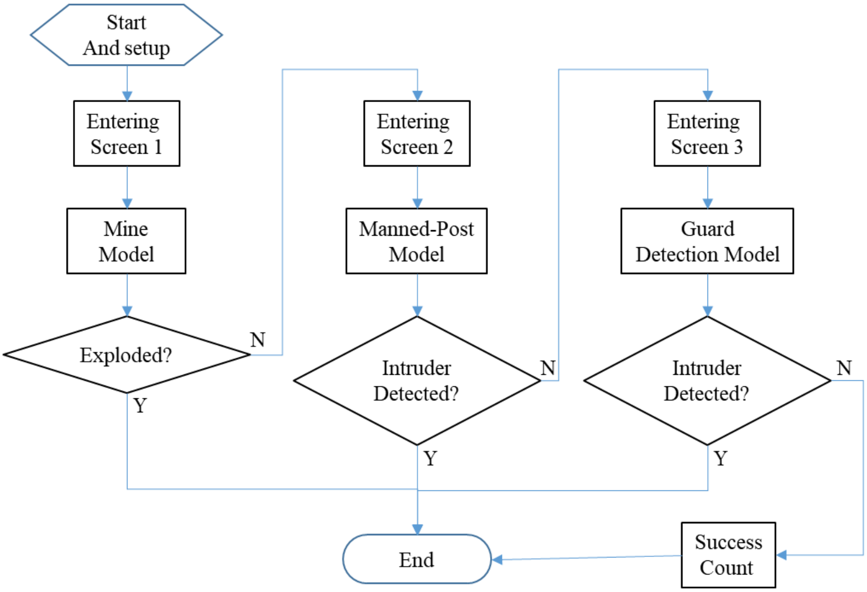
This specific scenario was designed to have the hostage held on a hilltop defended by a set up involving three alert screens to provide the terrorists with an early warning system which may gain them time to shift the hostage to another place if a penetration occurs. The concept of the terrorist's deployment is shown in Figure 1. The outer screen (screen 1) consists of landmines extending from the main entrance and with one sensor for detecting the penetrator. The explosion may deter the rescue squad and send back a loud and clear signal to the terrorists. The middle screen (screen 2) consists of manned posts in the middle of the hill. The last screen (screen 3) comprises the security guards who surround the building which is the terrorist's headquarters and where the prisoner is held hostage.

Figure 1 Depiction of scenario (see online version for colours)



In this scenario, there are two types of RSF with different equipment: the IoT-equipped and the not-IoT-equipped (conventional way).

Figure 2 RSF's penetrating operational logic (see online version for colours)



Based on the given scenario, the concept of the RSF operation is to aim to rescue the hostage held in the remote mountain area. A successful rescue mission is defined as the RSF penetrating all three screens. The logic starts with the initial setup such as the density of the landmines, the characteristics of the UAV and the terrorist security guards.

The following step is to check the chance of penetrating each screen. For screen 1, a landmine model would check that the rescue squad can penetrate with success; if not then the mission is counted as a failure. Screen 2 consists of several posts at specific points around the hill that will be checked by a manned post model for calculating the probability of detection. Screen 3 is the last resort for having the mobile security guard detection model to detect the penetrating rescue force. The logic flow is shown in Figure 2.

The scenario can be regarded as a simple set of three screens which create the probability of successful penetration for the RSF, i.e. P_i, i = 1, 2, 3. Screen 1 is the landmines laid by the terrorists to kill intruders, and it has a remote sensor for detecting intruders. A number of landmines extend from the two sides of the hill entrance, and they are uniformly distributed. Suppose the length of the landmine is L, the distance between two landmines is uniformly randomly distributed, the total number of landmines is N, and the effective width of the landmine to be initiated once stepped on is EW meters, such as in Figure 3. The effective range of the landmine in the simulation is depicted in Figure 4.

Figure 3 Concept of the laid landmine (see online version for colours)

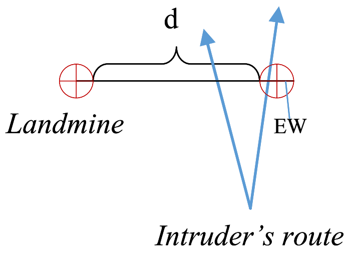
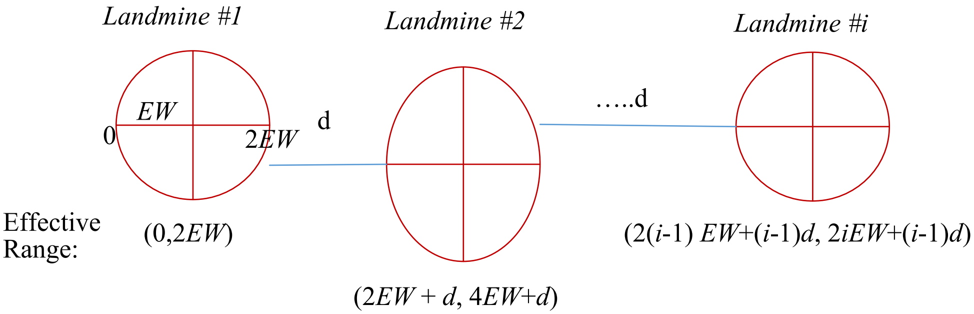


Figure 4 The effective explosion range for each landmine (see online version for colours)



The sensor of screen 1 has the probability of detection as $P_{d\_screen1}$, where the detection range is given in the simulation. Being killed by a landmine or detected by a sensor would count as successful in screen 1, which can be expressed by (1)

$$\begin{cases} =1, & \text{if } 1-\left[1-(i-1)(2EW+d)\le 2iEW+(i-1)d\right]*\left(1-P_{d\_screen1}\right) \\ =0, & \text{otherwise} \end{cases} \tag{1}$$

where, i is the sequence number of the laid landmine.

Screen 2 consists of a number of posts (NP) which are manned with thermal devices for watching the specific area which is depicted in Figure 5. The lateral range is defined by the 'cookie-cutter' approach in cell probabilities (Frost et al., 2001). The concept of using lateral range (LR) to form the sweep width of the watcher to determine the probability of detection is shown in Figure 6. The range in between posts is denoted by 2R. The probability of detection (P_{d_post}) as the RSF moves across the circle of the post in the simulation can be derived as (2)

$$P_{d\_post} = 1 - 2(R - LR)/R \tag{2}$$

Then, the count of detection by the post is as (3)

$$\begin{cases} = 1, & \text{if } P_{d\_post} > RAND() \\ = 0, & \text{otherwise} \end{cases} \tag{3}$$

Figure 5 The concept of deployment of posts in Screen 2 (see online version for colours)

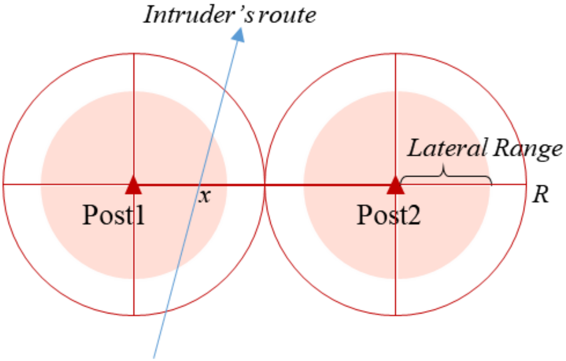
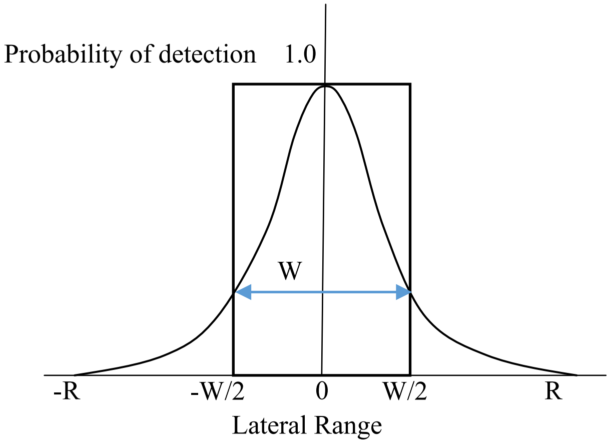
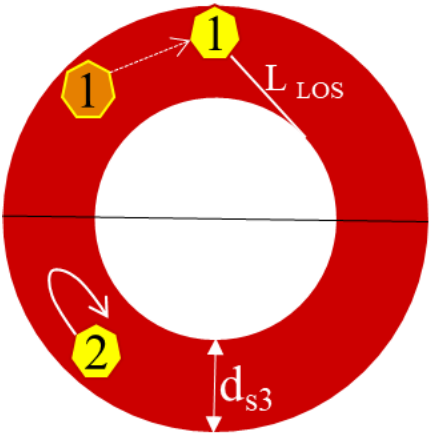


Figure 6 The lateral range and detection probability (see online version for colours)



(W: Sweep width)

Figure 7 The security check concept of Screen 3 (see online version for colours)



Screen 3 is the location next to the building where the hostage is held. The deployed secruity guards are moblised around the area. The terrorists are grouped as guards and are randomly spread out in the assigned sector for security checking around the building. The concept is shown in Figure 7. Assume that two groups share the circle's security check around the building. The parameters concerned include the width of the field to the building (d$_{s3}$), the moving speed of the guard (V_{Guard}) and RSF (V_{Squad}). Since, during the night, the thermal equipment is used, the guard has a line of sight (LOS) with a specific range. From end to end, the time for the guard to compelete the length of a half circle (L) check is $T_{complete\_L} = \frac{L}{V_{guard}}$. Under the LOS condition, the guard patrol on the perimeter of the circle is LOS to the building, which can save time. Assume that the range of LOS is LLOS, which is 1/n L, then the patrol range is $L(1 - 2/n)$. Then, the time to complete the patrol is shown in (4)

$$T_{complete\_L} = \frac{L\left(1-\frac{2}{n}\right)}{V_{guard}} \tag{4}$$

The RSF has to pass the field without being detected. In the simulation, the time starts to move across the field at time 0, and the time for crossing over the field is T_{cross_d}. If the distance between these two groups is greater than e L_{LOS}, then there would be no detection. Hence, randomised two points for both RSF and guard as ($Rnd\_location_{RSF}$, $Rnd\_location_{guard}$) represents both the location at the moment when RSF starts to cross, where $Rnd\_location_{guard}$ is no less than LLOS. The detection can be expressed as (5)

$$\begin{cases} = 1, & \text{if } L_{LOS} \geq Rnd\_location_{guard} - Rnd\_location_{RSF} \\ = 0, & \text{otherwise} \end{cases} \tag{5}$$

For the IoT-based RSF, due to the sensor network and unmanned systems being applied, much more data about the local situation, including detection of the hidden screens, can be acquired. After processing, those data become useful information, including the terrorist deployment and the detailed location of the landmines and posts. The decision support system (DSS) can then calculate the predicted penetration points and time needed to avoid detection by the deployed terrorists.

The UAV carrying GPR has been used in the detection of landmines. However, since there are no publications specifying the range of detection probability (Pd) in this situation, we assume that an error exists due to the possible missed detection. The error rate will be generated randomly within a given range. Mini drones are used to fly over the planned route to search for potential terrorists using the sensors on board, such as cameras and thermal sensors, which can provide a certain probability of detection of the object on land both during the day and at night. With mini drones in reconnaissance, the chance of the crossing RSF being spotted by the manned post is reduced due to the fact that the penetration route between the two posts is in a narrow range around the estimated least chance of the detected point. We express the route of penetration by normal random variable, i.e. $N \sim (\mu_{screen2}, \sigma_{screen2})$. The generated random number, which is a range x, if ($x + LR \geqq$ R) then RSF is detected. The range of x is changed when the sensor's error is taken into account. The last screen is with the guard patrolling around the building in which the hostage is held. The sensor on the mini drones, like a type of bug or little bird, can send the data about the terrorist guards, such as their location, patrol behaviour, and the number, back to the RSF. With the process in real time, RSF can identify the best timing to cross the field with minimum risk. The unpredictable uncertainty, i.e. a mistake made by the RSF, a sensor error or a sudden turnaround of the guard, is of concern in this crossing. It is described as a Uniform random variable such as $U \sim (0, UB)$, where UB is the upper bound of detection probability of the guard. The UB varies according to the integrated concern of the unpredictable uncertainty.

```
Algorithm of the simulation of RSF action
Begin
Initialise the setup of parameters and scenario.
Count1: conventional force
Count2: IoT-based force
  For $n$= 1 to simulation runs
    Conventional RSF
    'Enter screen 1
    If 1 – [1 – $Ratio\_Mine\_over\_field$] = (1 – $P_{screen1}$) > $Rnd$
    then
      Count1_screen1 = Count1_screen1+1
    Else
      'Enter screen 2
      Calculate $P_{d\_post}$ and generate Uniform random number ($Rnd$)
        If $P_{d\_post} > Rnd$ then
          $Count1\_screen2 = Count1\_screen2+1$
        Else
          'Enter screen 3
          If $L_{rand} \leqq L_{LOS}$ then
            $Count1\_screen3= Count1\_screen3+1$
          Else
            Count_RSF_success_conventional = Count_RSF_success_conventional + 1
          End if
        End if
    End if
    IoT-based RSF
    'Enter screen 1
    Generate Uniform random number limited in (0, maximum error), RSF_error_screen1
    If 1 – [1 – Ratio_Mine_over_field] = (1 – $P_{screen}$) * (1 – RSF_error_screen) > Rnd then
      count2_screen1 = count2_screen1 + 1
Else
      'Enter screen 2
  Generate normal random number, x, representing the possible error (range) made by sensors
  and human behaviour
      If (Probability_succeful_detection_conventional * sensor_error ≧ Rnd) then
        count2_screen2 = count2_screen2 + 1
    Else
        'Enter screen 3
        Calculate range between guard and RSF crossing point (RangeGuard_RSF)
          If RangeGuard_RSF ≦ $L_{LOS}$ then
            Count2_screen3 = Count2_screen3 +1
          Else
            Count_RSF_success_IoT = Count_RSF_success_IoT+1
          End if
      End if
    End if
  Next n
```

4 Analysis

The main objective of the analyses is to find out if there is a significant difference between the conventional and WoT-based RSF. In order to achieve that, we start with the assumptions which are required for matching the scenario. Then the cases representing the proper condition of the sensors are proposed. After running through the simulation model, the output data are presented for further analysis.

Following the given scenario and two major alternatives, i.e. the conventional and IoT-based RSF, some assumptions need to be made. In action, with extraordinary caution but without remote sensors, the conventional RSF would rely on their experience and instinct when trying to climb the hill to complete the mission. Taking advantage of IoT technology, before action, the IoT-based RSF is trained to wait until the collected data from the remote sensors are processed by the DSS in order to have the highest possible understanding of the terrorists' defensive setup and the suggestion of an accurate route. In light of the unknown performance of the sensors used by RSF which may cause errors, and for the purpose of finding if there is a significant difference among the various sensors, the parametric study is used in the study. The required assumptions are as follows:

- number of landmines: 30
- effective width to trigger the landmine (m): 0.2
- effective detection range of sensor in screen 1 (m): 50
- length of landmine field (m): 200
- the average lateral range of the manned post (m): 135
- range between the posts (m): 300
- responsible range of guard in screen 3: 50
- length of line of sight of terrorist guard (m): 20
- the possible error rate of the IoT sensors: 0.15, 0.3, 0.45, 0.6, 0.75
- landmine detection probability by RSF's UGS: 0.8
- IR sensor carried by UAV: lens/FOV with 19 mm/32° × 26°, operating temperature range from –21°C to + 50°C, a frame rate of 30 Hz, and operational altitude up to 3,048 m
- the definition of a successful task for the RSF is that they are undetected when crossing all three screens.

The error the sensor made can affect the task effectiveness. Therefore, this error is concerned in the study. The cases we are concerned with are the conventional and WoT-based RSF with UAV and UGS carrying sensors such as cameras and thermal sensors. The conventional RSF is case 1. The IoT-based RSF is classified into five cases based on the performance of the sensors, e.g. when the sensor's possible error is 0.15, 0.3, 0.45, 0.6, and 0.75. From the simulation of all cases, the results allow us to examine if there is a significant difference between the conventional and the WoT-based RSF.

The simulation results of all cases with each screen's detection or kill for failing the RSF in the conventional version and WoT_based is in Table 1.

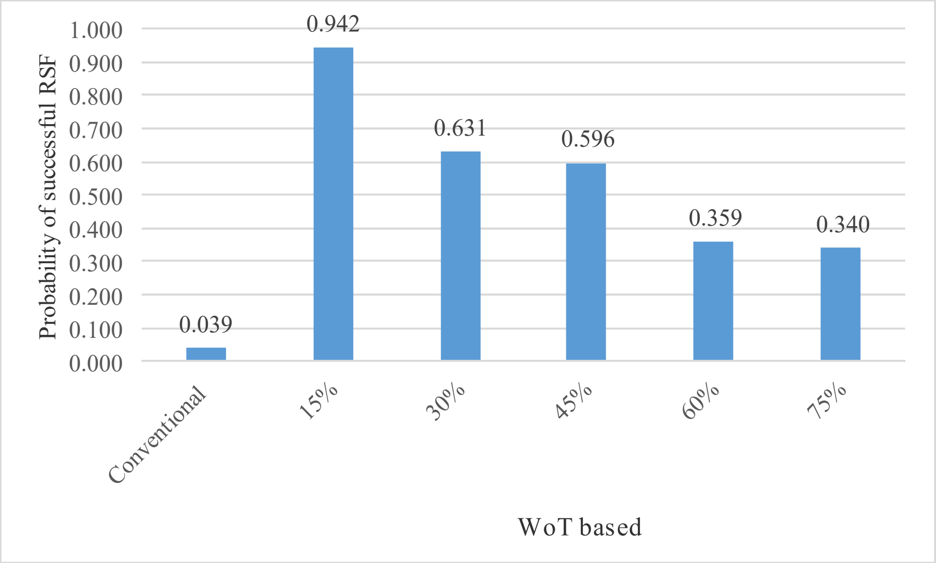
Table 1 The failure probability of RSF in crossing the screens setup by the terrorists

	Conventional	*WoT_based*				
		15%	*30%*	*45%*	*60%*	*75%*
Screen1	0.294	0.043	0.100	0.130	0.174	0.199
Screen2	0.629	0.111	0.215	0.335	0.436	0.514
Screen3	0.961	0.058	0.369	0.404	0.641	0.660

The successful probability of the RSF for finally penetrating all three screens is shown in Figure 8.

From the simulation results, it is obvious that the difference between the conventional and WoT-based versions is large. Even so, the question is how significant the difference is. Statistical tests on the simulation data were therefore performed.

Figure 8 The successful probability of the RSF in crossing all three screens (see online version for colours)



The *t* test shows that the p-values are 0.0492, 0.0368, 0.0497, 0.0342, and 0.0607 for the cases of 0.15, 0.3, 0.45, 0.6, and 0.75 vs. the conventional case, respectively. These p-values indicate that significant differences did exist in the cases of 0.15, 0.3, 0.45, and 0.6, but not 0.75. With one-way ANOVA to examine the different bias of sensors used by the WoT-based RSF, the result shows a p-value of 0.119, which is greater than 0.05, meaning the significance of those possible biases can be ignored as the task proceeds.

5 Conclusions

IoT is becoming increasingly popular in many areas; however, when the WoT is applied to integrating the IoT and sensors/objects, its effectiveness is clear. Police anti-crime work has always been the key to the safety and stability of society. Hence, the performance of the police in executing their tasks would be crucial with the consideration of time taken, risk of life and cost. One of the police tasks is to rescue hostages abducted by criminals, which has always been a tough problem for the government based on the historical records. The current police authority, for most of the countries, still lacks forward-looking strategies for modernising the current force, but they can take advantage of the advanced information technology. This paper provides a concept of WoT-based RSF as an alternative to the current approach taken by the police force in hostage rescue situations. Monte Carlo simulation and models were developed to analyze the effectiveness of these two alternatives. The results show that there was a significant difference between the two. The WoT-based RSF can provide more information about the situation to the command post than the current strategies, thus allowing the battlefield to be more transparent.

The greatest contribution of this paper is that it provides insights into how the hostage rescue task can be addressed using alternative strategies, and focuses on the effectiveness of taking advantage of advanced information technology. This information shows the significant effects that can support the decision-makers as a way of improving police performance when carrying out hostage rescue tasks.

A limitation of this study is that we focused on a very specific spectrum of police work; hence, it would be inappropriate to misuse this information for other police work. Therefore, the information is only suitable for this spectrum.

Our future work will be the study of more scenarios for obtaining further information to improve the concept of WoT-based RSF from various perspectives.

Acknowledgements

The author would like to thank the Ministry of Science and Technology for partially supporting this research under no. MOST-108-2221-E-032-036.

References

Abdelwahab, S.A.S. (2013) 'Efficient and safe wireless multi-sensor landmine detection system using image fusion through SC-FDMA transmission', *ITEE Journal*, Vol. 2, No. 4, pp.12–18.

Artyushenko, V.M., Volovach, V.I., Kartashevskiy, V.G., Neganov, V.A., Antipov, O.I. and Glushchenko, A.G. (2018) 'Determination of accumulating probability for norma distributions of range and detection efficiency of short range wireless devices', *ARPN Journal of Engineering and Applied Sciences*, Vol. 13, No. 2, pp.627–631.

Ashton, K. (2017) *Making sense of IoT*, Hewlett Packard Enterprise, California, USA.

Atzoria, L., Iera, A. and Morabito, G. (2017) 'Understanding the internet of things: definition, potentials, and societal role of a fast evolving paradigm', *Ad Hoc Network*, Vol. 56, pp.122–140.

Azuma, R.T. (1997) 'A survey of augmented reality', *Presence: Teleoperators and Virtual*, Vol. 6, No. 4, pp.355–385.

Cerquera, M.R.P., Montaño, J.D.C. and Mondragón, I. (2017) *UAV for Landmine Detection Using SDR-Based GPR Technology*, pp.272–329, Intech, London, UK.

Endsley, M. (2006) 'Situation awareness', in Salvendy, G. (Ed.): *Handbook of Human Factors and Ergonomics*, pp.528–542, John Wiley and Sons Press, New York City, USA.

Endsley, M.R. (1995a) 'Measurement of situation awareness in dynamic systems', *Human Factors*, Vol. 37, No. 1, pp.65–84.

Endsley, M.R. (1995b) 'Toward a theory of situation awareness in dynamic systems', *Human Factors*, Vol. 37, No. 1, pp.32–64.

Frost, J.R. and Stone, L.D. (2001) *Review of Search Theory: Advances and Applications to Search and Rescue Decision Support*, Soza & Company, U.S. Coast Guard Research & Development Center, Metron, Inc.

Green, M., Odom, J.V. and Yates, J.T. (1995) 'Measuring situational awareness with the 'ideal observer'', *Proceedings of the International Conference on Experimental Analysis and Measurement of Situation Awareness*, Florida, USA.

Gubbi, J., Buyya, R., Marusic, S. and Palaniswami, M. (2013) 'Internet of things (IoT): a vision, architectural elements, and future directions', *Future Gener. Comput. Syst.*, Vol. 29, No. 7, pp.1645–1660.

Guinard, D. and Trif, V. (2009) 'Towards the web of things: web mashups for embedded devices', *Proc. of the Second Workshop on Mashups, Enterprise Mashups and Lightweight Composition on the Web*, Madrid, Spain.

Hicks, J., Flanagan, R., Petrov, P. and Stoyen, A. (2003) 'Distributed augmented reality for soldier teams', *8th International Command and Control Research and Technology Symposium (ICCRTS'03)*, Washington D.C., USA.

Hodicky, J. and Frantis, P. (2009) 'Decision support system for a commander at the operational level', *Proceedings of the International Conference on Knowledge Engineering and Ontology Development*, Madeira, Portugal.

Kantorovitch, J., Niskanen, I., Kalaoja, J. and Staykova, T. (2017) 'Designing situation awareness: addressing the needs of medical emergency response', *Proceedings of the 12th International Conference on Software Technologies (ICSOFT 2017)*, Madrid, Spain.

Khan, M., Silva, B.N. and Han, K. (2017) 'A web of things-based emerging sensor network architecture for smart control systems', *Sensors*, Vol. 2, No. 17, pp.1–16.

Kusek, M. (2018) 'The internet of things: today and tomorrow', *41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, Opatija, Croatia.

Love, J. (2017) *The Truth About Range Data: How to Assess Thermal Camera Range Capability for Site Design Purposes*, DRS Technologies, Ottawa, Canada.

Lukosch, S., Lukosch, H., Datcu, D. and Cidota, M. (2015) 'Providing information on the spot: using augmented reality for situational awareness in the security domain', *The Journal of Collaborative Computing and Work Practices*, Vol. 24, pp.613–664.

MacDonald, J. and Lockwood, J.R. (2003) *Alternatives for Landmine Detection*, RAND Corporation, Santa Monica, CA, USA.

MacFarlane, R. and Leigh, M. (2014) *Information Management and Shared Situational Awareness*, Emergency Planning College Occasional Paper Number 12, Easingwold, UK.

Mahadevan, P. (012) 'The role of SWAT units', *IFS Insights*, No. 3, pp.1–23.

Mekni, M. and Lemieux, A. (2014) 'Augmented reality: applications, challenges and future trends', *Proceedings of the 13th International Conference on Applied Computer and Applied Computational Science (ACACOS'14)*, Kuala Lumpur, Malaysia.

Miller, E. (2016) *Annex of Statistical Information: Country Reports on Terrorism 2016*, National Consortium for the Study of Terrorism and Responses to Terrorism [online] https://www.state.gov/documents/organization/272485.pdf (accessed 28 January 2020).

Núñez-Nieto, X., Solla, M., Gómez-Pérez, P. and Lorenzo, H. (2014) 'GPR signal characterization for automated landmine and UXO detection based on machine learning techniques', *Remote Sensing*, Vol. 6, No. 10, pp.9729–9748.

Rajan, K.R.R.P., Prakash, J.A. and Selvan, S.T. (2014) 'Landmine detection using unmanned helicar', *International Journal of Innovative Science, Engineering & Technology*, Vol. 1, No. 3, pp.137–142.

Romanovs, U. (2016) *Digital Infantry Battlefield Solution*, Milrem Robotics, Tallinn, Estonia.

Roser, M., Nagdy, M. and Ritchie, H. (2018) *Terrorism*, OurWorldInData.org [online] https://ourworldindata.org/terrorism (accessed 28 January 2020).

Sun, J., Li, B., Jiang, Y. and Wen, C-y. (2016) 'A camera-based target detection and positioning UAV system for search and rescue (SAR) purposes', *Sensors*, Vol. 16, No. 11, pp.1–24.

Techopedia (2012) *Web of Things (WoT)*, Techopedia, 1 Februray [online] https://www.techopedia.com/definition/26834/web-of-things-wot (accessed 3 October 2019).

Timonen, J. (2018) *A Common Operating Picture for Dismounted Operations and Situations Room Environments*, National Defence University of Finland, Helsinki.

United States Department of Defense (2012) 'Common operational picture', *DOD Dictionary of Military and Associated Terms*, Washington, D.C.

Wickens, C.D. (1992) 'Workload and situation awareness: an analogy of history and implications', *Insight*, Vol. 14, No. 4, pp.1–3.

Wu, J-W., Chou, D-W. and Jiang, J-R. (2014) 'The virtual environment of things (VEoT): a framework for integrating smart things into networked virtual environments', *2014 IEEE International Conference on, and Green Computing and Communications (GreenCom), IEEE and Cyber, Physical and Social Computing (CPSCom)*, IEEE, Taipei.

You, X., Zhang, W., Ma, M., Deng, C. and Yang, J. (2018) 'Survey on urban warfare augmented reality', *Int. J. Geo-Inf.*, Vol. 7, No. 2, pp.1–16.