On Effective Campus Attack Response: Insights from Agent-Based Simulation for Improving Emergency Information Sharing System Design and Response Strategy

Steven Beattie1 · Jing Yang Sunny Xi1 · Wai Kin Victor Chan1

Abstract Information sharing systems are a critical component of emergency response—especially in campus attack situations that unfold very rapidly. The design of effective information sharing systems is often difficult, however, due to a lack of data on these assault events. This work takes an agent-based approach to simulate three campus emergency information sharing system design alternatives in the context of a college campus knife attack, and incorporates data from on-campus student surveys and parameter tuning experiments. Alternatives are evaluated according to: (1) improved student attack response outcomes; and (2) effective institutional response to the attack. The results confirm that increased awareness supports rapid emergency reporting, but an important gap exists between students’ awareness and their ability to respond effectively, which depends on a number of campus-specific factors. A strong positive impact is seen from safe and efficient information sharing with authorities. This impact depends largely on reporting system implementation qualities, as opposed to campus-specific factors. On a campus in China, WeChat was used as a basis for messaging models. The simulation results show a 9% drop in casualties and a 22% faster police response time from a text-based reporting system using “base” WeChat features instead of traditional phone reporting. Our results also project a 30% drop in casualties and 52% faster police response time using a system designed around a WeChat Mini Program or stand-alone campus emergency reporting app. These outcomes suggest a number of recommendations for improving outdated campus emergency information-sharing systems and response strategies.

Keywords Agent-based impact analysis · Agent-based modeling · Campus security · Emergency response · Information sharing

1 Introduction

Campus attacks are a part of emergency situations that can be difficult to study due to a lack of quantitative data regarding many aspects of how these situations unfold. At the same time, campus attacks are emergency events of increasing prevalence, and evidence-driven design for emergency response systems is a key area of research. Agent-based simulation provides researchers and emergency response planners with the ability to compare system design alternatives safely and efficiently. In this work, an example design comparison study was conducted for a university campus. The current emergency response system was simulated alongside two viable approaches to design improvement, and the results were compared.

1.1 Campus Emergency Response Systems

Around the world, many campuses effectively rely on social media platforms like Twitter and WeChat as de facto response system components. Despite technological advances, many response systems still include only telephone-based reporting and sparse, periodic Short Message Service (SMS)-based updates; this “hotline” based infrastructure is suboptimal for attack emergencies,
because the call is first sent to a call center and then directed to local law enforcement units (Salahshour 2015).

As messaging decisions become a large part of campus emergency response, social media platforms are increasingly used by students to fill in the information gaps left by current systems. Such phenomena are seen in Twitter use in response to other types of emergencies (Thomson et al. 2012; Abedin and Babar 2018), and in the “false alarm” example seen at the University of Michigan in 2019 (Washington Post 2019). In the case of campus attack response, which relies heavily on timely information sharing and efficient information processing, social media platforms may be a poor substitute for dedicated emergency response infrastructure.

Yabe (2017) argues that mobile campus safety apps could provide advantages over traditional blue light emergency towers by allowing students to efficiently notify campus police while staying hidden from attackers. Romano et al. (2016) suggest that the wide array of functionalities and the ubiquity of modern cell phones can transform users into “human sensors” with GPS, Wi-Fi, accelerometer, camera, and so on. In the University of São Paulo, an app that enables users to share their GPS locations and provide other relevant information when they report to the police has reduced the response time from 8–10 to 5–7 min (Ferreira et al. 2017). Vaghela (2015) has proposed a campus security app on smartwatch that provides location-based emergency notification. Testimonials from users showed that the wearable app provided more convenience, security, and willingness to use than existing local emergency notification systems. It has been noted that, in China, a WeChat Mini Program may provide similar functionality to stand-alone apps, on a platform which is already familiar to users and which may be particularly desirable to school and public officials due to the link with the trusted “base” WeChat platform.

1.2 Agent-Based Simulation

Though little work has been done using agent-based modeling for system design analysis, many researchers adopt agent-based models to explore human behaviors during emergency response. Okaya and Takahashi (2011) incorporated psychological models of agent behavior (for example, Belief-Desire-Intention) into an evacuation model. Zhang et al. (2018) examined evacuation during violent attacks in open public space. Ma et al. (2017) considered response to a sarin gas attack in a railway station. Briggs and Kennedy (2016) explored the risks and benefits of fighting back during an attack. Other studies have focused on-campus attacks specifically. Anklam et al. (2015) have considered the possibility of encouraging “concealed carry” of firearms on campuses. Xi and Chan (2019) modeled the different dynamics and outcomes between a gun attack and a knife attack on the same campus. In most previous work, however, the influence of message system design on attack response outcome has not been explored.

Beattie et al. (2020) have simulated information sharing using WeChat, the most popular messaging app in China, between students during a knife attack. In this work, the effects of available message types on campus-wide event awareness and response outcomes were explored via agent-based simulation and compared to outcomes produced without messaging. The study found that messaging can reliably increase on-campus awareness of an attack; this leads to faster reporting times, and thus a quicker end to the attack, compared to results seen without using messaging capabilities. The results showed that the increased awareness produced by messaging may have a positive impact on response outcomes, and that group-based messaging is expected to produce the largest benefit despite potential trust issues. However, the analysis was limited only to the campus’ current information sharing system design, and the influence of the emergency reporting system was not considered.

Emergency reporting and on-campus messaging are both important aspects of campus emergency response. In this study, we considered the impact of three different campus emergency response system designs suggested by previous studies. The three scenarios are: (1) WeChat-based messaging and phone-based reporting (Salahshour 2015), which serves as the baseline model of the current campus; (2) a text-based reporting system using a basic group chat or WeChat Official Account (Beattie et al. 2020); and (3) a WeChat Mini Program, or a stand-alone campus emergency reporting app (Ferreira et al. 2017; Yabe 2017). Scenarios 2 and 3 both consider the introduction of emergency alerts and improved message notifications, but frequency varies by scenario according to potential functionality options. The alternative system design scenarios modeled in Scenarios 2 and 3 represent promising design pathways that could improve baseline performance; they can be described as “maximizing utility of current messaging platform-based infrastructure,” and “utilizing a purpose-built, app-based emergency response infrastructure,” respectively.

To assess the potential effectiveness of these design improvements, we used an agent-based simulation of a knife attack on a college campus in China. A model representation of WeChat was used for communication between students, and data from on-campus student surveys were incorporated into parameter tuning. The response strategy and message evaluation models are extensions of the work presented in Beattie et al. (2020). In this work, the prevalent “Run, Hide, Tell” response...
strategy (Metropolitan Police Service 2017) was implemented to model student decision making. The model minimizes the assumptions made about students’ decision-making context, leading to a strategy implementation that is appropriate for the variety of circumstances that students may face. The message evaluation model for students considered the time, content, and source of incoming messages. A variety of tests were conducted on each of these three scenarios and key metrics were recorded, including the amount of casualties and police response time. The effectiveness of security and community response were evaluated and attributed to specific response system components. Finally, recommendations are proposed for improving response system design based on these results, and opportunities for follow-up work are discussed.

2 Methods

An agent-based model is implemented using NetLogo software and programming language to simulate a hypothetical knife attack scenario on a university campus in China. The node-based simulation environment is defined to coincide with a GIS map of the campus (Fig. 1). Buildings on the map include dormitories (green), laboratories (blue), lecture halls (orange), and canteen (brown). The attack takes place in the lecture halls, which are three connected buildings.

Three types of agents are simulated; these include 1 knife-wielding attacker, 3000 students, and 2 police officers. The numbers of student and police agents are chosen to reflect current circumstances on the university campus examined in this study. To reduce the complexity of the knife attack scenario, a single attacker is initialized, and casualty is defined according to the production of “injury,” as opposed to “fatality.” Based on empirical on-campus estimation, 80% of students are placed inside buildings while 20% are dispersed among “outside” nodes to simulate a mid-afternoon attack during a normal school day. Two police officers (black star) and one knife attacker (red triangle) are spawned at set locations. Police agents are stationed at two police office locations on campus, and the attacker’s location can be set by the user. During simulation, each time step of the model (or “tick”) represents 5 s, which is approximately the time needed for an agent to move from one node to another in the physical, real-world campus space. When the attacker is subdued by the police, the simulation ends.

2.1 Simulation Validation and Parameter Tuning

Since there is a severe lack of validation data for these kinds of attacks, we rely heavily on the validity of survey results and modeling assumptions to ensure that the study results provide a sufficient level of accuracy in reflecting expected system behavior. Unless otherwise stated, probabilistic events are modeled using a Bernoulli (0.5) distribution, since data are still lacking on many aspects of campus emergency response. This is done in order to facilitate experimentation and greater understanding of expected system behavior, while making the least number of assumptions possible with respect to distributional characteristics. Some parameters that can be tested in everyday circumstances were tuned using basic trial experiments among a small group of students; these parameters include message composition time, message checking time, and report form filling times. Evaluation of conflicting message information is assumed to take place instantaneously and does not extend a student’s decision making or action duration in the current model.

In future work, parameter tunings may be improved using expanded experimental trials in which a larger number of samples and data points may be collected from decisions and feedback produced in a hypothetical attack scenario. The current work provides a “proof of concept” for integrating survey and experimental data collection into the development of emergency response strategies and related infrastructures.

2.2 Attacker Agent Rules

The attacker has three Attack Destinations and spends a minimum of 2.5 minutes at each destination. The attack path is drawn in red on Fig. 1. The minimum of 2.5 minutes per attack destination is chosen to facilitate the production of a reasonable attack rate overall. We estimate that an average of one attack every 10–11 s (cf. Zhang et al. 2018 who also modeled knife attacks) may be reasonable, given the physical layout of the campus studied, the proximity of attack locations chosen for simulation, and the premise that the attack takes place during the regularly-scheduled afternoon classes that take place inside of the buildings on campus chosen for attack.

If students are present at the attacker’s current location but the attacker is not at an attack destination, there will be a 50% chance that the attacker moves. Simulations run with this tuning produce the estimated attack frequency. If no students are present, then the attacker will continue moving along the shortest path to the next attack destination. If there is no remaining attack destination, a random move is chosen.

Additionally, at each tick when an action is not already being executed, the attacker must make an action choice between “move” and “attack.” Each action takes 10 s to complete, and there is a 50% probability for each choice. If “attack” is chosen, the success probability is set to 100%
unless the student chosen is “hiding” (represented as a 75% chance of not being discovered; if not discovered, another student is “chosen” to attack) or in the process of “running” (represented as a 25% reduced chance of attack success). The attacker is assumed to have full knowledge of the campus layout but does not have access to the messaging system.

2.3 Student Agent Rules

Survey results from Beattie et al. (2020) were used in parameter tuning, as the previous work is recent and the same campus is studied here. Follow-up survey questions were asked for this study and are included in Table 1.

2.3.1 Unalerted Students

At the start of each simulation, all students are unalerted. The attacker begins the attack, and students become alerted to the attack in one of two ways: (1) direct presence at the attack location; or (2) receipt of a message about the attack from someone else. The first carries a 50% chance of alert; the second carries a 100% chance of alert. For instance, under condition (1), if a student has been on the attack location for 2 ticks, he or she has a 75% chance to be alerted. Action choices for unalerted students are “move” and “stay” and are given 50% probability each essentially an unbiased coin toss. “Move” takes 10 s, while “stay” lasts 5 s.

Unalerted students check their messages according to the time distribution described in the survey results in Table 1. An unalerted student can also become alerted upon receipt of a message. Messages can come from friends, groups, or a central authority. WeChat users generally have a vast number of contacts, which are gathered in a wide variety of different scenarios; in the modeled environment, however, each student has three friends based on survey results of mean 2.6 in Table 1.

2.3.2 Alerted Student Action Choices

Five action choices are considered: “run,” “hide,” “tell (texting),” “tell (reporting),” and “freeze” (Fig. 2). “Run” takes 5 s to complete and moves the student to the next map node. When running, students will take the shortest path to their randomly chosen destination. “Hide” can only be chosen while a student believes that he or she is on the attack node. While hiding, the student may choose to “tell” (send a message, or report if available, but no phone calls) or simply hide. The student will hide until he or she learns

---

Footnote:
1 These reductions (for Hiding, Running, and Alerting) are hypothetical, and are not currently based on real-world data. However, current sensitivity analysis shows that these parameters make little difference in the current environment.
that the attacker has moved away from their location; at that point, the automatic action choice is to "run." Students’ messages sent via the "tell (texting)" action go to a friend or the group chat. According to empirical testing, message sending time is randomly distributed between 5 and 40 s (approximated by uniform distribution). No messages are sent with malicious intent, and all students assume their current information to be true. Students executing "tell (report)" use their currently believed attack location, and report submission time varies by scenario. To prevent "spamming," students may only file one report per location.

In an attack situation, few people are truly prepared to act without hesitation. Each time a student has a choice to make, there is a possibility that he or she will hesitate, or "freeze up." In the model, the "freeze" action lasts for one simulation step. The inclusion of a "freeze" possibility also helps to differentiate students in their response speed, to reflect the fact that some students may respond to the situation more or less swiftly than others.

In every attack situation, there is a possibility that a student will choose to fight back. The decision to fight back (or not) is complex and is not addressed here (cf. Briggs and Kennedy 2016; Xi and Chan 2019).

### 2.3.3 Decision-Making Strategy Modeling

The decision-making model implements a “Run, Hide, Tell” response strategy and is designed to avoid assumptions on the scenarios in which students will be making decisions. Students are assumed to be logical, level-headed, and make action choices based on a rational perception of their situation. This is a large assumption, but implies that student actions are interpretable as rational best-choices given their contextual information at the time. Action

| Info Requested                                      | Student Responses |
|-----------------------------------------------------|-------------------|
| Number of close friends on campus                  | 2.60 (Mean)/1.96 (Std Dev) |
| Time taken to respond to friend’s messages          | 0–30 s: 31        |
|                                                    | 30–60 s: 34       |
|                                                    | 1–2 min: 37       |
|                                                    | 2–5 min: 23       |
|                                                    | 5–10 min: 18      |
|                                                    | > 10 min: 22      |
| Number of big WeChat groups (≥ 100 group members)  | 0: 2              |
|                                                    | 1–5: 70           |
|                                                    | 6–10: 51          |
|                                                    | 11–15: 22         |
|                                                    | 16–20: 9          |
|                                                    | 21–25: 3          |
|                                                    | 26–30: 3          |
|                                                    | > 30: 5           |
| Muted all group chats (no real-time notification enabled) | 44.24%          |
| Not knowing the campus security number             | 79.39%           |
| Report incident to police before warning friends   | 66.67%           |
| Perceive text-based reporting as safer than phone-based | 100%            |

![Diagram](image)
probabilities here should be interpreted as a representation of the general preference for a given action over another under the modeled response strategy. Adverse outcomes can be credited to either a lack of contextual information leading to a suboptimal decision, suboptimal execution of the decision produced, or the result of a student encountering a lose-lose situation.

→ Run vs. Tell: If a student has time to “tell,” he or she also may have time to attempt an escape, and vice versa. The decision between these options may reflect how safe the student feels taking the time to “tell,” or their desire to communicate. The “run” action is modeled as 2x more likely, reflecting strategy-recommended preference ordering.

→ Run vs. Hide (if “run” is chosen): After choosing to “run,” a student will consider whether “hide” may in fact be a better choice. This decision depends on a variety of contextual factors and is modeled here as an unbiased Bernoulli(0.5) distribution in order to avoid assumptions about students’ decision-making circumstances.

→ Report vs. Text (if “Tell” is chosen): The student will need to decide between texting and filing a report. If the simulation scenario requires phone reporting, a report cannot be made at the attack location; this reflects the recommendation made in prominent response strategies including “Run, Hide, Tell.”

2.3.4 Information Sharing Model

Today, WeChat is by far the most used messaging and social networking app in China. It is currently a de facto piece of national infrastructure that is used every day by the state, businesses, universities, and individuals for a wide array of purposes. Therefore, the campus messaging system is modeled after WeChat, which has many features including friend and group messaging.

Students can send private messages or group messages, but only one message of each kind may be sent per location to avoid “spamming.” The group chat modeling implies a fully-connected group communication network with equal weights between each node. For the campus studied, this is an appropriate model due to the very high level of interconnectedness between students and the high number of large group chats in use on campus.

2.3.5 Message Evaluation Model

Messaging assumptions: Perfectly clear messages are always sent; students are always honest (that is, no disinformation); a friend’s word is considered more strongly than a nonfriend’s; the security office is assumed to be “specialized” in assessing a situation; the security office is perceived to be honest and transparent; central messages are as accurate as the current monitoring and response infrastructure allows.

The message check is executed quickly between 5 and 15 s with uniform distribution based on empirical tests. Students may check messages in a variety of situations—periodically, before texting others, when hiding, and so on. In the model, students will place emphasis on the latest reliable information. Accordingly, messages are separated according to their source: group, friend, or central authority. The attack location most frequently cited in the most recent simulation step is accepted. For example, in a list of messages [ 1 2 2 3 3 3 ], location “3” will be adopted as latest information. But if the message list is [ 2 2 2 3 3 3 ], messages citing locations “3” and “2” are in conflict. In the event of such a “tie,” the authority of messages’ sources is compared, and the most credible source’s message is adopted. For simplicity, a central message (that is, emergency alerts and updates) is trusted over friends’ messages, which are trusted over messages from the group chat.

2.4 Police Agent Rules

Report Processing: Once the police agents receive a report, they process the information and mobilize a response immediately. As officers mount their response, new reports are continually being processed and integrated into police agents’ situational awareness. Reports are held in a first-in-first-out queue, and one report is processed at a time. Report processing time varies by scenario.

Central Messaging: In Scenario 2, emergency alerts are released after a report is finished processing. However, in Scenario 3, an emergency alert is generated automatically upon receipt of a report, reflecting the system configuration on many campuses. Alert messages always contain the most up-to-date information held by the security office. Subsequent updates may also be periodically sent after an emergency alert.

First Responder (“Police”) Activity: When a report has been processed, police agents are immediately dispatched to the reported attack. They take the most direct route to the currently believed attack location and have two action possibilities: “move” and “neutralize attacker”; each action take 5 s to complete. Police agents choose “move” until the attacker is found. In this study, we assume that police fully engage and neutralize the attacker when they find the attacker; extenuating circumstances, such as a protracted standoff, are not modeled here. When found by police, the attacker is neutralized and the simulation ends.
2.5 Simulation Flow, Objectives, and Scenario Design

The simulation flow is illustrated in Fig. 3. The objective of this study is to evaluate the impact of emergency information sharing system design on campus attack response outcomes and derive insights on how the system design can be improved to support better expected response outcomes in a campus attack scenario. Specifically, we evaluate the impact of a standard system design in comparison to two design alternatives according to a number of evaluation metrics.

System designs are separated into three scenarios (Fig. 4). Scenario 1 is the “baseline” system design that utilizes phone-based reporting; Scenario 2 is an improved system design that utilizes text-based reporting via WeChat’s group chat or Official Account features; Scenario 3 is a second improvement scenario that considers app-based reporting via WeChat Mini Program or a standalone campus emergency app. Comparison of these three scenarios provides insights to several questions that, taken together, play a large role in effective campus emergency information sharing system design. For example:

Does student to student information sharing support improved outcomes in any scenario?
Do emergency alerts/updates provide benefits beyond student to student information sharing?
Can text-based reporting systems out-perform phone-based systems?
Can significant additional benefits be expected from an app-based system, versus a social media-based system?
Given that the three directions of information sharing in this model, students to students, students to authorities, and authorities to students, are dependent on each other, does any one of these options yield a larger response impact?
Does “Run, Hide, Tell” adequately address information-sharing decisions in attack response, considering the information-sharing system design alternatives presented here?

Scenario 1 reflects the baseline response scenario as it currently exists on campus. It features emergency phone calling and basic end-user WeChat messaging functionality (friend messages and group messages). Approximately 80% of students on campus cannot contact the campus security office directly, reflecting survey results (Table 1) regarding student unawareness of the campus security phone number. In order to report an attack, these students will need to call a local emergency-reporting number instead. This means that more time is needed to submit a report. The reporting method has implications for when a report can be made safely, how long it takes to make a report, and how long a report takes to be processed.

The first set of optimizations are modeled in Scenario 2 and reflect optimizations that could be made by more fully utilizing the functionality available on the “base” WeChat messaging platform—for example, group chats or a WeChat Official Account. This approach may be relatively simple to implement and uses an already-adopted platform that users are familiar with and implementation may not require the deployment of additional technology. On the other hand, certain functionality that may be desirable for an emergency messaging system may be unavailable or difficult to implement with “base” platform functionality.

The optimizations modeled in Scenario 3 address some of the shortcomings present in Scenario 2, while still retaining its benefits over Scenario 1. Emergency response apps are already used to handle emergency reports and alerts/updates on many university campuses around the world. In China, WeChat Mini Programs may provide a way to implement stand-alone app functionality while also utilizing the “base” and “back-end” functionality of the already ubiquitous WeChat platform. In both cases, the app or mini-program could be integrated with campus video monitoring systems, which are already established on many campuses around the world (Ferreira et al. 2017; EdTech Magazine 2019). In the United States, adoption is already over 96% (Campus Safety Magazine 2019). Coordination between video monitoring and app-based resources could allow for a highly streamlined response on the part of security authorities.

In an emergency response app or mini-program, reporting could be enhanced by various features like geolocation (increase speed, clarity, and accuracy of location reporting), effective multimedia integration, client-side report form storage (reduced time needed to access, and by extension submit, a report form), and background operations (for features like real-time Emergency Updates). Consistent real-time emergency updates could be made available to the community through the app as well, with significantly improved campus security personnel actionability.

2.6 Simulation Execution and Evaluation Metrics

Simulations of each scenario were conducted in order to: (1) Evaluate the effectiveness of current attack response infrastructure; and (2) Compare two important design approaches to response infrastructure improvement.

Nine evaluation metrics are used in the current study, which are presented in Table 2. Results are calculated from the mean ending values (for each evaluation metric data point) collected from simulations in each scenario, and are presented in Fig. 5. For each data point, the standard deviations of repetition results were relatively low. In future work, as the simulation and data analysis platform becomes more developed, the potential for unpredictable outcomes in a given modeling scenario may be better integrated into results assessment.

In Fig. 5, subplots 1–9 correspond to the evaluation metrics presented in Table 2; 300 simulation repetitions were conducted for each scenario. In subplots 1–3, the minimum, mean, and maximum observed values are plotted; in subplots 4–9, mean values are used for scenario comparison. In subplot 2, no value is displayed for Scenario 1 due to the absence of central messaging capability described in Sect. 2.5 and Fig. 4.

3 Results and Discussion

Simulation results largely confirm qualitative assessments of emergency response needs that are already known to campus security experts. For example, simulation results illustrate the importance of quick and safe community reporting in an emergency, the ability to quickly process incoming reports, and the value of well-designed emergency alerts in producing effective community response
measures. But how can we describe the marginal value of a dedicated emergency app, versus a form-based approach that may be embedded in already-adopted communication platforms, for example, or the ability of a form-based approach to improve on the baseline campus-specific response system? As described in Sect. 2.5, these are some of the questions that this introductory study is intended to help answer, as well as to assist explanation of the dynamics behind the answers.

### 3.1 Results Comparison across Scenarios

For Scenarios 1, 2, and 3, average casualties were 32.64, 29.60, and 22.56, respectively. In the current simulation, the three attack locations are adjacent classroom buildings with the attacker starting in building 1. In Scenario 1, the attacker often completes the three-location attack, and proceeds to randomly attack students while roaming around campus. In Scenario 2, the attacker is frequently stopped en route to building 3, after completing attacks on buildings 1 and 2. In Scenario 3, the attack is usually ended before the attacker can complete the attack on building 2.

The average attack durations are 7.38, 6.00, and 4.52 min, respectively. The use of an emergency app in Scenario 3 reduced the police response time by almost 3 minutes, versus phone-based reporting in Scenario 1, which is consistent with Ferreira et al. (2017). In Scenario 1, attacks usually last long enough so that more than 2/3 of students on campus have received notification of the attack. In Scenario 2, approximately 55% of students become alerted, while in Scenario 3, approximately 1/3 of students become alerted.

Results demonstrate that the “baseline” emergency response infrastructure (social messaging platform for information sharing, emergency reporting by phone, infrequent SMS Emergency Updates) has significant room for improvement. Both improved infrastructure design approaches simulated here provide better results across all dimensions of evaluation, but Scenario 3 provides the best response efficiency and overall response outcomes out of all three scenarios. Simulation data show a 9% drop in casualties and 22% faster police response time when using online reporting (Scenario 2) instead of traditional phone reporting (Scenario 1), and a 30% drop in casualties and 52% faster police response time when using a campus emergency app-based system (Scenario 3).

If the investment necessary for a system in Scenario 3 cannot be secured, system improvements along the Scenario 2 design pathway may provide a lower-cost way to improve on a “baseline” response system, if further utilization of already-adopted communication platforms is a possibility. WeChat provides this possibility via Official Accounts, but currently the vast majority of its user base is in China, and platforms commonly used outside of China (for example, WhatsApp or Twitter) currently do not have equivalent functionality available. If WeChat adoption is deemed undesirable on campuses outside of China, improvement options based on Scenario 2 may be limited, and improvement options based on Scenario 3 will require development of a new system or adoption of a new platform.

A system based on the Scenario 3 design pathway of purpose-built, coordinated emergency response infrastructure that utilizes modern technologies (for example, emergency app and campus monitoring) may provide considerably better results. According to the current data, a Scenario 3 system provides better results across all metrics, improving information dissemination, security reporting and report processing, and overall response efficiency—leading to meaningfully reduced attack times and casualties.

### Table 2 Evaluation metrics for use in knife-attack scenario simulations

| Metric Name                      | Definition                                                                 |
|---------------------------------|-----------------------------------------------------------------------------|
| (1) Simulation length           | How long did the attack last before the attacker was stopped?                |
| (2) 1st central message         | If the information-sharing system supports emergency alerts and updates, how long did it take to generate the first emergency alert? |
| (3) Police mobilization time    | How quickly were police mobilized to respond to the attack?                 |
| (4) Number of casualties        | How many students were attacked (injured)?                                  |
| (5) Number of students alerted  | How many students were aware that there was an attack taking place?         |
| (6) Number of locations checked by police | How many destinations did police agents check before finding the attacker? |
| (7) % of casualties alerted     | How many casualties had been alerted to the attack?                        |
| (8) % of casualties alerted with correct info | How many alerted casualties held an accurate and up-to-date belief about the attacker’s current location? |
| (9) Number of attacker location changes | How far was the attacker able to move before being stopped by police? |
3.2 Message-Based Improvement

Student to student messaging was expected to increase student awareness of the attack and help students maintain an updated awareness as the situation unfolds. This, in turn, was expected to support students’ ability to escape or avoid the attack location more effectively, and the effect was expected to be magnified with earlier emergency alerts and more frequent emergency updates. Results show that awareness was increased, confirming results from the literature.

The rate of casualty accumulation remains unchanged even in Scenarios 2 and 3, holding at approximately 5 casualties per minute in each scenario. In order for this rate to fluctuate, locations in the attacker’s pathway would need to be fully evacuated. Based on the current models and these results, we can see that this may be a high bar to meet. In any case, only a small number of students need to remain in an attack area in order for the casualty rate to remain unchanged.

In every scenario, 82–85% of casualties had already been alerted to the attack, and 90–96% of students were correctly informed about the attack (Fig. 5). While accurate and earlier alerts may lead to earlier reliable reports, this did not lead to sufficient opportunity to act effectively on communicated information; as a consequence, a large enough number of students remained at each attack.

Fig. 5 Simulation results for all three scenarios and nine evaluation metrics in on campus knife-attack study
location (and along the attacker’s pathway) for the rate of casualty accumulation to remain constant.

With central messages providing accurate information earlier and more often, along with the increasing levels of correct situational awareness among student casualties, one can infer that student to student messaging and emergency alerts may potentially help students form a more effective response via supporting sustained accurate understanding of the situation as it unfolds. Although many students may have been able to escape attack or avoid the attack location, enough students were still present at the attack locations for the attacker to maintain a consistent rate of attack across all scenarios. This result approximates real-world circumstances in which, for example, the physical layout of the attack location, or the number of students present, may prevent students from effectively escaping the immediate vicinity of the attacker. While this situation may not arise on all campuses, it may be highly location-specific. This is an important possibility for system designers to consider, as in these cases information sharing may not directly benefit students in the vicinity of the attacker.

3.3 Report-Based Improvement

While increased awareness did not necessarily lead to improved attack avoidance, improved reporting systems produced a consistent and significant improvement in student and institutional attack response outcomes. This impact depends largely on system implementation, and integration with other emergency response systems on campus (for example, video monitoring). The benefit of a well-designed reporting system may not depend strongly on campus-specific factors like physical space design, number of students present, and so on, and response improvements stemming from improved reporting system design may be more robust against variations in these factors; in other words, the effectiveness of reporting systems can be expected to be relatively consistent across a variety of campuses.

Due to subsequent improvements in reporting and report processing times in Scenarios 2 and 3, the average time that security officers mobilized to respond was 3.78 minutes and 2.31 minutes, respectively, down from approximately 4.84 minutes in Scenario 1. Furthermore, average variation in mobilization time is reduced from ±1 minute by 16% and 42% in Scenarios 2 and 3, respectively. The between-scenario trends in mobilization time mirror those seen in attack length and number of casualties, and in police response efficiency (Table 2). As mobilization time is reduced, and response efficiency is increased, simulation length decreases proportionally and the number of casualties is reduced as well.

The modeled video monitoring system integration in Scenario 3 produces an increase in response efficiency as well. In Scenarios 1 and 2, responding police agents depend on continued and accurate community reporting to ensure that they are en route to the correct attack location. In Scenario 3, however, police maintain correct knowledge of the current attack location, presumably due to utilization of a campus video monitoring system. This design change allows police to arrive at the correct attack location every time; in Scenarios 1 and 2, police reach at least one wrong location, on average, before making their way to the correct location. This adds to the response time and allows further casualties to accumulate. These results suggest that reporting systems with campus video monitoring capability may provide meaningful support for security response efficiency.

Notable response improvements produced in this study primarily arise from giving students the ability to provide an emergency report quickly and quietly to campus authorities and supporting authorities’ ability to quickly process and respond to these reports. Such tools can be developed in the context of a campus emergency app, or an already-adopted messaging platform (if the platform has appropriate functionality). Both may provide improvement, but the capabilities afforded by a stand-alone app may be more beneficial than a social media app for campus emergency response purposes.

3.4 General Results, Observations, and Recommendations

Regardless of the design pathways used, our work highlights the importance of improving on the so-called “baseline” campus emergency response systems. From the current results, broadly applicable recommendations for improving campus emergency information sharing system design can be made. These recommendations are categorized into three directions and should be confirmed by further campus-specific design impact analysis before adoption.

(1) Fast and safe emergency reporting and report processing systems are critical. For reporting efficiency, app-based reporting should be preferred over phone-based as currently designed and employed. The phone-based reporting system effectively restricts students from reporting when they’re away from the attack location; phone-based reporting may be inefficient, but also may benefit individual students’ safety. If electronic reporting is available, students will need clear and effective guidance on safe reporting practices. In addition, utilizing app-based features such as cookies and geolocation, which
may expedite form filling and reporting within an app, may also help in developing effective semi-automated report processing.

2) **Timely and sufficiently-detailed emergency alerts and updates should be prioritized as well.** Effective emergency alerts and emergency updates, combined with efficient reporting and report processing, may help eliminate the need for continued information sharing between students.

3) **Campus safety experts should determine how much info sharing should be left to emergency alerts.** Student to student information sharing takes time and may expose students to an attacker. On the other hand, students will inevitably worry about their classmates’ safety. Community information sharing has been consistently shown to have a positive impact on response outcomes, but the level of direct benefit may vary considerably across campuses. If reporting and report processing happens quickly, emergency alerts and updates may take the place of most student to student messages—supporting more efficient student responses without potentially leaving students unaware. As decisions of when and how to share information with others are increasingly becoming a part of everyday life, campus safety experts need to address and guide these decisions in their recommended response strategies (while distinguishing “texting” from emergency reporting).

### 4 Conclusion and Future Work

Information sharing is an important aspect of modern emergency response scenarios. The current work builds on recent studies that explore the impact of information sharing in the context of campus attack scenarios. In our work, de facto and intentionally designed emergency response infrastructure are evaluated with regards to their impact on student and police response outcomes, using an agent-based simulation environment designed based on previous work and real-world data.

Results demonstrate considerable room for improvement in the “baseline” campus emergency response system, which represents systems still used in many places around the world. This “baseline” system suffers from relatively slow information dissemination and reporting times, resulting in longer attacks and more casualties. Although an online reporting system produces improvement in these metrics, a dedicated app-based reporting system produced considerably better results in the current simulations. Student to student messaging and emergency alerts do not demonstrate a significant, direct impact on students’ ability to avoid attack if these students are in close proximity to the attacker. The reporting system is found to be the biggest factor in community response effectiveness. While student to student messaging and emergency alerts increase student awareness (and thus expedite emergency reporting), their direct benefit to students is expected to vary according to specific circumstances around the attack location. Many questions remain for future work, which may further inform the design of improved campus emergency response systems.

This study only examines information dissemination, does not consider auditory communication, and approximates group chats with one large group. Addressing these factors may result in improved realism in results. Also, scenarios could be considered in which the attacker is part of school staff, or even a security officer on campus (ChinaDaily 2020). Agent differentiation may also be important, for example, simulation of unique staff and student agents. Such work could help to test systems designed for use in primary and secondary schools, which have become frequent targets as well (CBS News 2019; New York Times 2019). As authorities play an increasingly leading role in information dissemination, concerns about the effect of suppressive local policies towards information sharing should be considered. The potential detrimental effects of reduced information sharing in the campus community are shown in Beattie et al. (2020). If students are afraid or unwilling to share, for example, due to fear of unpredictable or negative repercussions from security officials, then student and security response efficiency both may suffer. Another important route for future work is campus-specific system design, and further testing of specific response system features, for example, blue light emergency posts, or using an emergency alert similar to the America’s Missing: Broadcast Emergency Response (AMBER) Alert (Wikipedia 2022). A variety of different response strategy formulations are used around the world, as well; further research may examine the efficacy of personal response strategy recommendations given to the campus community.

**Acknowledgments** This research was funded by the Shenzhen Science and Technology Innovation Commission (JCYJ20210324135011030, WDZC20200818121348001), Guangdong Pearl River Plan (2019QN01X890), and National Natural Science Foundation of China (Grant No. 71971127).

**Open Access** This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article’s Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article’s Creative Commons licence and your intended
use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

References

Abedin, B., and A. Babar. 2018. Institutional vs. non-institutional use of social media during emergency response: A case of twitter in 2014 Australian bush fire. Information Systems Frontiers 20(4): 729–740.

Anklam, C., A. Kirby, F. Sharevski, and J.E. Dietz. 2015. Mitigating active shooter impact: Analysis for policy options based on agent/computer-based modeling. Journal of Emergency Management 13(3): 201–216.

Beattie, S., J.Y.S. Xi, and W.K.V. Chan. 2020. Evaluating aspects of WeChat use for information sharing during a campus attack event using agent-based simulation. Journal of Physics: Conference Series 1621(1): Article 012078.

Briggs, T.W., and W.G. Kennedy. 2016. Active shooter: An agent-based model of unarmed resistance. Proceedings of the 2016 Winter Simulation Conference, 11–14 December 2016, Arlington, VA, USA, 3521–3531.

Campus Safety Magazine. 2019. 2019 video surveillance survey: Campus cameras more popular than ever. https://www.campus-safetymagazine.com/research/2019-video-surveillance-survey/. Accessed 1 Sept 2021.

CBS News. 2019. 8 killed in latest attack targeting school children in China. https://www.cbsnews.com/news/china-school-attack-in-hubei-leaves-8-elementary-school-children-dead-today-2019-09-03. Accessed 1 Sept 2021.

ChinaDaily. 2020. Security guard stabs 39 at Guangxi primary school. http://global.chinadaily.com.cn/a/202006/04/WS5e8d87184a310a8b24115ae3a.html. Accessed 1 Sept 2021.

EdTech Magazine. 2019. Behind the scenes: The hardware behind keeping campuses safe. https://edtechmagazine.com/higher/article/2019/09/behind-scenes-hardware-keeping-campuses-safe-percon.com. Accessed 1 Sept 2021.

Ferreira, J.E., J.A. Visintin, J. Okamoto, and C. Pu. 2017. Smart services: A case study on smarter public safety by a mobile app for University of São Paulo. In Proceedings of 2017 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation, 4–8 August 2017, San Francisco, CA, USA, 1–5.

Ma, L., B. Chen, S. Qiu, Z. Li, and X. Qiu. 2017. Agent-based modeling of emergency evacuation in a railway station square under sarin terrorist attack. International Journal of Modeling, Simulation, and Scientific Computing 8(2): Article 1750022.

Metropolitan Police Service. 2017. Staying safe from terrorism. https://www.met.police.uk/advice/advice-and-information/terrorism-in-the-uk/staying-safe-from-terrorism. Accessed 1 Sept 2021.

New York Times. 2019. Attack at school in China leaves at least 8 children dead. https://www.nytimes.com/2019/09/03/world/asia/china-attack-school.html. Accessed 1 Sept 2021.

Okaya, M., and T. Takahashi. 2011. Human relationship modeling in agent-based crowd evacuation simulation. In International Conference on Principles and Practice of Multi-Agent Systems (PRIMA 2011): Agents in Principle, Agents in Practice, 14–19 November, Wollongong, NSW, Australia, 496–507.

Romano, M., T. Onorati, I. Aedo, P. Díaz. 2016. Designing mobile applications for emergency response: Citizens acting as human sensors. Sensors 16(3): Article 406.

Salahshour, C. 2015. Emergency response system. U.S. patent application publication. Publication US 2015/0038109 A1. Washington, DC: U.S. Patent and Trademark Office.

Thomson, R., N. Ito, H. Suda, F. Lin, Y. Liu, R. Hayasaka, R. Isochi, and Z. Wang. 2012. Trusting tweets: The Fukushima disaster and information source credibility on Twitter. In Proceedings of the 9th International Conference on Information Systems for Crisis Response and Management (ISCRAM), 22–25 April, Vancouver, Canada. Simon Fraser University. http://www.robithomosensors.com/wp-content/uploads/2012/04/Thomson_et_al_2012_Trusting_Tweets.pdf. Accessed 14 May 2022.

Vaghela, S. 2015. WalkSafe: College campus safety app incorporating Pebble Smartwatch. Master’s thesis. Pennsylvania State University, University Park, PA, USA.

Washington Post. 2019. University of Michigan campus shooting false alarm. https://www.washingtonpost.com/national/false-alarms-real-fear-even-without-gunfire-active-shooter-alerts-create-terror/2019/03/19/1f7f66d7f8-4a55-11e9-b79a-961983b7e0cd_story.html?arc404=true. Accessed 1 Sept 2021.

Wikipedia. 2022. Amber alert (America’s Missing: Broadcast Emergency Response). https://en.wikipedia.org/wiki/Ambert_alert. Accessed 5 May 2022.

Xi, J.Y.S., and W.K.V. Chan. 2019. Simulation of knife attack and gun attack on university campus using agent-based model and GIS. In Proceedings of the 2019 Winter Simulation Conference, 8–11 December 2019, National Harbor, MD, USA, 263–272.

Yabe, M. 2017. Cost-benefit evaluation: Students’, faculty’s, and staff’s willingness to pay for a campus safety app. Journal of Criminal Justice Education 28(2): 207–221.

Zhang, F., S.C. Wang, and Z.H. Song. 2018. Evacuation during violent attacks: Agent-based modeling and simulation. In 2018 IEEE 9th International Conference on Software Engineering and Service Science (ICSESS 2018), 23–23 November 2018, Beijing, China, 412–415.